



**DECISION
OF
THE COMMISSION FOR PERSONAL DATA PROTECTION
REG. №. ПАИКД-13-28/2023
SOFIA,.....**

The Commission for Personal Data Protection (CPDP, the Commission), composed of Chairman [REDACTED] and members [REDACTED], [REDACTED] and [REDACTED], at a meeting held on 7 February 2024, examined and discussed a notification with ref. No. ПАИКД-13-28/20.07.2023 of a personal data breach under Article 33 of Regulation (EU) 2016/679. BOROVETE I AD, (the company, the controller), submitted the notification. In connection with a "medium level of risk" found, according to the "Methodology for risk assessment of personal data breach", adopted by the Decision of the CPDP of Protocol No. 35/29.09.2022, a documentary check was carried out on the controller. A Finding Report was issued with reference No. ПАИКД-13-28#26(23)/05.02.2024, containing detailed findings regarding the inspection.

I. Factual background

By letter with ref. No. ПАИКД-13-28/20.07.2023 notification of a personal data breach under Article 33 of Regulation (EU) 2016/679 was received from the Controller BOROVETE I AD, Company No. (UIC): 204605689, having its headquarters and registered office in Varna, Primorski District, Postal Code 9006, Sts. Constantine and Helena Resort, administrative building, whose scope of business is: hotel and restaurant management, tour operator and travel agency services, domestic and foreign excursion arrangement, leisure events. In addition, a letter with ref. No. ПАИКД-13-28#5/14.08.2023 was submitted to clarify the facts of the case.

II. Initial analysis of the breach notification and actions taken

1. Nature of the breach

The notification under Article 33 of Regulation (EU) 2016/679 states that on 18 July 2023 the Controller identified a data breach when a responsible employee of the hotel's Reservations Department (Aquahouse Hotel & SPA) found out that a large number of messages have been received to the Company's account on Booking.com. Those messages were received in response to 'phishing' communications to customers concerning reservations made. At the same time,



telephone calls have also been received concerning the nature of this message and inquiries whether payments were due in respect of current and/or pending reservations. As a result of the breach, phishing messages were sent to hotel customers. The message sent to the individuals (translated into several languages depending on the nationality of the message addressee) contains a fraudulent warning of current or future customer reservations if they fail to confirm their payment card details on a redirecting malicious link sent for this purpose.

According to information provided to the Controller by the IT Security Department of Booking.com the unauthorised access was made through the account of the Company's Executive Director with the username [REDACTED]

A person who had made a reservation to stay in the hotel contacted a staff member of the Reservations Department asking for assistance in the transfer from the airport to the hotel. In the course of the correspondence, this person sent a file containing information that the employee should have used for the transfer. The employee started a file entitled 'Additional information about the reservation.exe', which contained a malicious code.

The password of the Company's Executive Director for Booking.com was revealed through the infected file, and such password was probably used to access her account and have illegal correspondence with Company's customers.

Citizens of the following countries are affected by the breach: Bulgaria – 4, Romania – 47, Poland – 1, Canada – 1, Russia – 1, Ukraine – 3, Sweden – 1, Switzerland – 1, Türkiye – 1, UAE – 1, Israel – 1, Italy – 6, Germany – 1, UK – 8.

People who replied to the phishing message are from Bulgaria – 1, Poland – 1, Israel – 1, Italy – 1, Russia – 1, Ukraine – 1, Germany – 2, Romania – 12.

The categories of personal data affected by the breach are: names, nationality, e-mail address, telephone number, and with respect to people who replied to the phishing message information about their bank payment card, bank and/or payment account were also affected.

2. Actions taken by the Controller to limit and prevent further breach

- Following the identification of the unauthorised access to the Company's business account on Booking.com, measures have been taken to change passwords and means of authentication to Aquahouse Hotel & SPA account;
- The devices used by the Company for access were scanned for malware;
- Email passwords were changed;
- An additional specialised antivirus program was installed;



- A standard of operation and automation of a dynamic change of passwords (30 days of activity) was introduced;
- Additional initial staff training at the start of employment was foreseen;
- EDR system (Endpoint Threat Detection and Response System) was integrated; the IT Unit will monitor the system on a 24/7 basis and will respond to breakthrough alerts;
- The persons affected by the breach were notified.

The initial analysis of the information in the notification is contained in Report No. ПАИКД-13-28#6/11.09.2023. The level of risk to the rights and freedoms of data subjects was determined in accordance with the ‘Methodology for assessing the risk of a personal data breach’ adopted by CPDP Decision in Protocol No. 35/29.09.2022. There is a ‘medium risk’ to the rights and freedoms of the affected individuals. At a meeting, CPDP adopted the following decisions:

1. Carry out a documentary check of the Data Controller.
2. To constitute CPDP as the lead supervisory authority, as the Controller’s main or single establishment is located in the territory of the Republic of Bulgaria (Article 56 (1) of the Regulation);
3. To register the case in the Internal Market Information System (IMI), specifying that CPDP is the lead supervisory authority and to provide brief information on the breach and the nationalities of the affected EU citizens. The procedure is initiated by the CPDP on 26 September 2023 and is registered in the Internal Market Information System (IMI) under number IMI 560753. The supervisory authorities of Rhineland-Palatinate, Italy, Romania, Berlin, Bavaria and the Netherlands have identified themselves as concerned supervisory authorities. On 17 April 2024, the Commission for Personal Data Protection published in IMI a draft decision in relation to Notification No. ПАИКД-13-28/20.07.2023 submitted by the controller BOROVETE I AD. No reasoned and relevant objections were raised by the deadline for the submission of objections (expired on 15 May 2024) by the concerned supervisory authorities.

III. Analysis of the documents and opinions submitted in connection with the inspection

In order to fully clarify all the relevant circumstances of the case, additional information was requested from BOROVETE I AD by letter with ref. No. ПАИКД-13-28#10/02.10.2023.



By letter with ref. No. ПАИКД-13-28#14/23.10.2023, the Controller provided the requested information.

In connection with the breach, additional information was also requested from Booking.com by letter ref. No. ПАИКД-13-28#19/15.12.2023. Booking.com provided the requested information via IMI through the Dutch supervisory authority, by a letter with ref. No. ПАИКД-13-28#24/19.01.2024.

The Controller specifies that the personal data protection is ensured in accordance with the requirements of Regulation (EU) 2016/679. The guidelines, opinions and recommendations of the European Data Protection Board and the implementing decisions of the European Commission are observed.

In accordance with the requirements of Article 24(2) of Regulation (EU) 2016/679, the Controller has adopted an Instruction (internal rules) on measures and means to protect personal data collected, processed, stored and provided by Borovete I AD. Privacy Policy and Information Security Policy have also been approved.

The Information Security Policy is part of the internal corporate documentation approved for the purposes of ensuring the compliance of the Company's activities with the requirements arising from European and national regulations in the field of personal data protection, as well as the best practices in the field of cybersecurity. The staff has been familiarized with the Information Security Policy and with other internal corporate documents. A copy of such documents has been sent to the heads of all Company's departments and thus all employees have been informed of the objectives and texts of the internal documents adopted. The heads of departments are, in their turn, engaged to bringing the corporate documents adopted, including the Information Security Policy, to the attention of the staff. The Controller has provided evidence that the employees are familiar with internal corporate documents.

The Controller has developed an instruction to regulate the creation of accounts on online tour operator platforms, and such instruction shows which employees may have accounts on online platforms used by the Controller.

The organisation in the company is set up so that employees of the Reservations Department have their own profiles on the online platforms they use.

The heads of departments carry out the overall monitoring of compliance with the obligations arising from all internal orders and instructions.

The control of compliance with the internal rules and procedures for dealing with accounts and passwords is also carried out directly by all the staff in the IT Department, who have software generating log files allowing real-time tracking of all processes carried out by the Company's



computers. In this regard, all employees of the Company's IT Department report to the head of department any irregularities detected in the use of data, including unauthorised access from a personal computer to accounts of other employees with other computers, including through access to third-party service providers platforms.

The Controller reports that access to information assets is provided on a need-to-know basis, and that access control is carried out directly by the heads of departments. The overall business of the Company complies with this principle.

All databases containing personal data are accessed only by employees expressly authorised by the Executive Director of the Company and solely for the performance of their duties.

The Company's employees work through individual accounts with individual passwords for the computer and system devices, with no access to the data files of any other employee, department, or access to PCs or internal accounts of other employees in the same or other department. The creation of these accounts ensures the proper functioning of the Company's business operations involving tourist accommodation and the provision of hotel services to customers.

All employees of the Company are informed of compliance with this principle as soon as they start working in the relevant department or in the event of changes in the Company's policies.

It is clear from the information provided by Booking.com that when partners register on the platform, they are given access to the Extranet on Booking.com, where they can manage all matters concerning their facility, such as room prices, room availability, discount offers, reservations made, the partner's contact details, adding or deleting 'trusted devices' allowed to enter the Extranet, etc. The Extranet allows a partner to communicate directly with the guests via a partner-guest communication tool and to see selected personal details of guests who made a reservation with that partner. A partner does not have access to the guest's email address via Extranet, but only to the alias of the guest's email address. Access to the Extranet is provided to partners on a need-to-know basis and partners are informed and contractually bound to keep their login credentials secret. Access to Extranet is protected by technical and organisational security measures such as mandatory two-factor authentication, which cannot be disabled. It is possible to create accounts with different access rights so that to ensure that certain actions can only be performed by Extranet users having root privileges. These are the so-called 'child accounts' (subaccounts). Child accounts are accounts linked to the partner's main Extranet account, but have their own username and password. Passwords are required to include a minimum of 10 characters, including upper and lower case letters and digits.



When a new session is started, Booking.com requests the Extranet user to authenticate itself by two-factor authentication at least once every 15 days. In addition, Extranet sessions have a life of 7 days in an active session or 2 hours when they are inactive; this means that every 7 days or 2 hours, depending on the activity of the session, the partner may be required to log in again.

As a result of the internal investigation, Booking.com identified ten ‘child accounts’ in the Extranet account of the partner Aquahouse Hotel & SPA, all such accounts having root privileges. It can therefore be inferred that the Controller has not taken action to limit the powers of its staff to the Extranet account.

In this case, it can be concluded, and this was confirmed by Booking.com, that following the start of the malicious executable file, the person acting maliciously obtained access to information in the partner’s web browser during a session where the partner had already entered its account by means of two-factor authentication. Subsequently, the person acting maliciously used the compromised account and sent messages on behalf of the Controller requesting payment card data to be provided to a relevant redirecting malicious link.

The Controller reports that data to which the Company and its authorised employees have access on Booking.com are the client’s name and reservation details (stay, type of room, number of guests). The storage, including retention periods for personal data of Company’s customers on Booking.com, is determined by the rules of the platform, and Company’s employees have only single access to the data accessible on the platform after the performance of their hotel accommodation duties. In this context, the Company stores no data of its customers on Booking.com after their reservation is made.

Booking.com states that customers’ personal data are stored in partners’ accounts as follows:

- For the time prior to the date of accommodation of the person who made the reservation and during the stay of this person in the partner’s accommodation facility;
- The alias of the email address of the person who made the reservation is subject to deactivation two months after the departure date. Partners may send communications only from the moment of booking to seven days after the departure date or seven days after cancellation;
- Customer’s personal data are not displayed on the partner’s Extranet after 30 days from the departure date.



Booking.com also states that following the investigation it was established that the person who acted maliciously had not accessed credit card data from the Controller's Extranet account.

The Company's internal inspection did not identify any damage or abuse of the personal data of the customers who communicated with the unauthorised person.

All affected hotel guests were duly accommodated. No person has made any claim, in law or in fact, against the hotel. All guests were addressed with compliments by the team of Aquahouse Hotel & SPA, their reservations were prepaid via the Booking.com platform, and the latter has not reported any information about clients' claims or claimed damages.

The Controller reports that the Company's organisation with regard to the collection, storage and processing of personal data is as follows:

Physical protection:

- Only authorised staff of the department to which the computers have been made available have physical access to the individual computers. This means that the computers in the Reception Department are only accessible by staff of this department by means of an individual password of each employee;
- Aquahouse Hotel & SPA has a security alarm system, a video surveillance system, a back-up power supply, a fire alarm and fire protection system, air conditioning of the premises where hardware devices are located;
- The Company has a personal data breach response team;
- Access to all hotel rooms, staff entrances, administrative offices, parking areas and the premises in which the hotel server is located is controlled;
- The hotel managed by the Company has 24/7 physical security and an electromechanical hotel patrol system.

Personal protection:

- The Company's employees have appropriate personal data protection training;
- When dealing with external providers, verification of the identity of the person who will provide the service in question;
- Personal protection measures include access to personal data only by persons whose duties or specifically assigned tasks require such access, subject to the “need-to-know” principle;
- Arrangements and measures are in place to prevent disclosure of information to third parties;



- The levels of access to the different categories of personal data are regulated and differentiated by the approved Instruction;
- The staff members sign a declaration of non-disclosure of personal data to third parties.

Documentary protection:

- Access to personal data records is governed and regulated by an instruction;
- For each of the personal data registers a retention period is set which complies with the relevant regulatory requirements;
- A procedure is in place for the destruction of personal data in paper and electronic form.

Protection of automated information systems and/or networks:

- The Company's network is not specifically certified in terms of information security. However, under the approved rules, the Company uses technical devices and software which is in line with international standards;
- Access to the Company's IT systems is regulated through usernames and passwords, and the different accounts have different levels of access;
- The software products used by the Company allow logging of access and actions carried out, and any act of entering, modifying, deleting data from hotel customer registers can be traced;
- Archives are produced at operating system and file level;
- Measures have been taken to ensure the reliability and integrity of the systems: back-up power supply of servers, isolation of the server from the internet database, separation of the physical integrity of servers in separate, dedicated double-locked premises, separation of network into segments;
- Rules are in place for regular technical maintenance of computer equipment and systems;
- The Company uses TLS cryptographic protocols for its email customer, thus ensuring the confidentiality, integrity and authenticity of the data;
- The Company has also configured the maintenance of TLS cryptographic protocol for its web server;
- All platforms and software used by Company's employees apply control by time-limiting user sessions;



- Some of the Company's employees use external connectivity to databases through VPN;
- The process of creating copies and back-ups (autosave) is automated at server and storage level (storage sites);
- Destruction, deletion and erasure of data carriers by designated staff members is controlled by the implementation of a specific Procedure for destruction of personal data in paper and electronic form.

The Controller states that it has notified all persons affected by the breach.

It is found that within 72 hours of becoming aware of the breach, the Controller notified the supervisory authority, the CPDP, in accordance with Article 33 of Regulation (EU) 2016/679.

All the documents provided by BOROVETE I AD for the purposes of the inspection were enclosed in case file with ref. No. ПАИКД-13-28/20.07.2023.

IV. Legal analysis:

Regulation (EU) 2016/679, which applies as of 25 May 2018, is the legal act laying down rules on protection of personal data of natural persons with regard to their processing. The Regulation builds on the former data protection regime introduced by Directive 95/46/EC, transposed into the Bulgarian Personal Data Protection Act of 2002, while taking into account the dynamics of the development of new technologies and of personal data processing activities.

According to the legal definition set out in Article 4(12) of the Regulation, a '*personal data breach*' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The specific breach consists of starting a malicious executable file by a Controller's employee, resulting in a third party having accessed the Executive Director's account on Booking.com. This shows the employee's insufficient awareness and caution, despite the training on data protection. In addition, the Controller has not taken sufficient technical and organisational measures to limit the access rights of its employees on Booking.com, although this platform provides such limitation as an option, and thus the third party has easily accessed the account of the Controller's Executive Director. Personal data of 80 (eighty) persons were affected by the breach: names, nationality, email address, telephone number, including financial data of 20 (twenty) natural persons who replied to the phishing message such as details of a bank payment card or bank account or account with a payment service provider. In this case, Article 5(1)(f) of Regulation (EU) 2016/679 has been infringed, namely the data were processed in a manner that



fails to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, subject to the principle of ‘confidentiality’.

On the other hand, as mitigating circumstances, it should be taken into account that the Controller notified the CPDP without undue delay, within 72 hours of becoming aware of the breach. Data subjects are informed by email. Additional actions have been taken to prevent such incidents by installing an additional specialised antivirus program, actions to ensure additional initial training for new hires, and EDR system (Endpoint Threat Detection and Response System) has been integrated.

It is the responsibility of the Controller to take the appropriate technical and organisational measures to protect data and to apply mechanisms to monitor the implementation of such measures, and thus the Controller could demonstrate compliance with the rules of the Regulation.

CPDP has a margin of discretion, in accordance with the powers entrusted to it, to determine which corrective powers referred to in Article 58(2) of Regulation (EU) 2016/679 to exercise. The assessment is based on considerations of appropriateness and effectiveness, taking into account the specificities of each individual case and the extent to which the interests of the specific data subjects are affected, as well as the public interest. The powers referred to in Article 58(2), other than that under subparagraph (i), have the nature of coercive administrative measures designed to prevent or put an end to a breach, thereby achieving proper conduct in the area of personal data protection.

When applying the appropriate corrective measure under Article 58(2) of the Regulation, account shall be taken of the nature, gravity and consequences of the breach, as well as any mitigating and aggravating circumstances. The assessment of what measures are effective, proportionate and dissuasive in each individual case also reflects the objective pursued by the chosen corrective measure of preventing or putting an end to the breach or penalising the unlawful conduct, or both, as provided for in Article 58(2)(i) of Regulation (EU) 2016/679.

Having regard to the facts of this case and the results of the documentary check which unequivocally confirmed the facts and circumstances of the case, taking into account the nature, gravity and consequences that could arise from the data breach, and after reviewing and analysing all the documents gathered in the administrative case file, and in order to prevent further such breaches, the Commission for Personal Data Protection adopted the following



DECISION:

1. Pursuant to Article 58(2)(b) of Regulation (EU) 2016/679, for breach of Article 5(1)(f) in conjunction with Article 32(1)(b) and (d), issues a **reprimand** to BOROVETE I AD in connection with notification of a personal data breach under Article 33 of Regulation (EU) 2016/679 with ref. No. ПАИКД-13-28/20.07.2023.
2. Pursuant to Article 58(2)(d) of Regulation (EU) 2016/679, for breach of Article 5(1)(f) in conjunction with Article 32(1)(b) and (d) of Regulation (EU) 2016/679, **orders** the Data Controller BOROVETE I AD to:
 - 2.1 Take actions to restrict the rights of its employees on Booking.com, in order to comply with the ‘need-to-know’ principle; and
 - 2.2 To draw up a plan for periodic training of employees in the area of personal data protection, including points concerning phishing messages. Periodic phishing drills should be conducted to increase employees’ vigilance.

The order under paragraph 2.1 shall be complied with **within 1 (one) month from the entry into force of the decision**, after which, within 14 (fourteen) days, the Controller shall notify the Commission for Personal Data Protection of its implementation by submitting the relevant evidence.

The order under point 2.2 shall be complied with **within 3 (three) months from the entry into force of the decision**, after which, within 14 (fourteen) days, the Controller shall notify the Commission for Personal Data Protection of its implementation by providing relevant evidence, including the training materials to be used for the training.

This Decision of the Commission for Personal Data Protection and may be appealed against before Varna Administrative Court within 14 (fourteen) days of its receipt.

CHAIRPERSON:

[Redacted signature]

MEMBERS:

[Redacted signature]

[Redacted signature]

[Redacted signature]

[REDACTED]
Management board member

Your: 07.05.2020

Our. 14.08.2020 nr 2.1.-1/19/4601
[REDACTED]**Notice of termination of the proceeding in regard to the protection of personal data**

The proceeding of the Estonian Data Protection Inspectorate concerned the claim of a Lithuania citizen [REDACTED] (complainant) in regard to the fact that the [REDACTED] transferred the personal data of the complainant about his dept to [REDACTED], without informing about debt.

Given the above, we initiated a supervision proceeding on the basis of clause 56 (3) 8) of the Personal Data Protection Act.

In its response to the inquiry from the Estonian Data Protection Inspectorate, [REDACTED] stated that it did not violate the Personal Data Protection Act or the General Data Protection Regulation, but acted in accordance with the laws and the contract concluded with the client.

During the proceeding, [REDACTED] stated the following:

1. *The complainant was a client of [REDACTED], who ordered the service of [REDACTED] by concluding a service provision contract with [REDACTED] on 06 January 2007. On 18 August 2009, [REDACTED] terminated the contract with the complainant due to a debt. [REDACTED] processes the appellant's personal data (name, surname, address, telephone number, and personal identification code) based on the concluded contract and law in order to perform the contract and recover the debt.*
2. *On 16 September 2019, [REDACTED] forwarded the complainant's personal data to [REDACTED] in accordance with the contract concluded with the [REDACTED].*
3. *Clause 11.3 of the contract concluded with the client highlights that [REDACTED] has the right to transfer, without the consent of the client, its contractual rights and obligations to third parties, provided that the transfer does not violate the client's rights. The client's rights have not been violated, as upon conclusion of the contract, it was agreed that the client will receive the service and [REDACTED] will be paid for the service provision. If the debt for the service remains unpaid, the service provider has the right to demand the payment of debt that the client had to take into account when concluding the contract. The same option is also provided in subsection 164 (1) the Law of Obligations Act, establishing that an obligee may transfer the claim thereof to another person on the basis of a contract in part or in full regardless of the consent of the obligor (assignment of claim). A claim shall not be assigned if assignment is prohibited by law or if the obligation cannot be performed for the benefit of any other person but the original obligee without altering the content of the obligation. The client*

- failed to pay the debt, after which [REDACTED] transferred the debt to a person processing debts, and in this case, to [REDACTED] for debt recovery purposes.*
4. [REDACTED] offers credit management services. As [REDACTED] entered into an agreement with [REDACTED], then the new creditor and the data controller is [REDACTED].
 5. [REDACTED] has had the right to transfer the personal data to [REDACTED] in accordance with the agreement with the client and law (in point 3). On 23 October 2019, [REDACTED] informed the complainant that [REDACTED] had transferred the complaint's personal data to [REDACTED], therefore the new creditor and the data controller is [REDACTED].

[REDACTED] has explained to the Estonian Data Protection Inspectorate that it received the complainant's data in connection with the conclusion of a contract with him for the use of the service and shall process such data to perform the contract – for debt recovery purposes.

As the complainant failed to pay the debt, his details were transferred to the [REDACTED] with whom [REDACTED] had a debt collection contract.

Information that [REDACTED] may transfer the complaint's data to third parties without his consent has already been communicated to the complainant upon conclusion of the contract (clause 11.3 of the contract). It is clear from the response of [REDACTED] that the complainant was notified by [REDACTED] on the transfer of the debt on 23 October 2019.

The Estonian Data Protection Inspectorate also explains that with regard to processing of personal data, it only assesses whether the transfer of personal data has been lawful, not the lawfulness of the debt claim. The Estonian Data Protection Inspectorate does not have the competence to assess whether the debts of individuals against the creditor have arisen lawfully, what the claims consist of, whether or not the debt has actually been liquidated, whether or not the rules for the assignment of the claim have been complied with, as those are disputes that arise from contractual relations. Settlement of contractual disputes between private parties is a matter for the civil court.

As [REDACTED] has received personal data from the complainant at the time of concluding the contract and [REDACTED] processes such data lawfully (for the purpose of concluding and performing the contract) and the complainant has been informed of the transfer of personal data or the possibility thereof, we find that the processing of the complainant's personal data was lawful. Therefore, we shall terminate the supervisory proceeding.

Respectfully

/signed digitally/
[REDACTED]

Senior Inspector
authorised by Director General

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: the '**GDPR**');

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework (hereinafter: the '**Law of 1 August 2018**');

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 07AD/2024 of 23 February 2024 (hereinafter: the '**ROP**');

Having regard to the Procedure for complaints before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the '**Complaint Procedure before the CNPD**');

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or **GDPR**), the Supervisory Authority of Brandenburg (Germany) submitted to the National Data Protection Commission (hereinafter: "the **CNPD**") a complaint (national reference of the concerned authority: 136/22/0398) via IMI in accordance with Article 61 procedure - 416588.
2. The complaint was lodged against the controller [REDACTED], [REDACTED] (hereafter "**[REDACTED]** who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated that the complainant alleged that he was the owner of a [REDACTED] account he did not use for several years. He wanted to use it again and was asked by [REDACTED] to provide it with the last four numbers of the banking account linked to his account, in order to verify his identify and reset his password. Unfortunately, the complainant did not remember it anymore as it is a more than ten years old bank account. The situation with [REDACTED] was blocked and the complainant decided to request the deletion of his account.

4. In essence, the complainant asked the CNPD to request [REDACTED] to close his or her [REDACTED] account and delete any related personal data.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and to provide a detailed description of the issue relating to the processing of the complainant's personal data, in particular with regard to his or her request for erasure. Moreover, the CNPD required [REDACTED] to proceed to the deletion of the complainant's personal data as soon as possible, unless legal reasons prevent the former from doing so.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. Pursuant to Article 17 GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17(1) GDPR applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17(3) GDPR.
10. Furthermore, in application of Article 12(2) GDPR "*the controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 GDPR emphasises that "*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means.*"

11. Article 56(1) GDPR provides that “*(...) the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60*”;
12. According to Article 60(1) GDPR, “*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other*”;
13. According to Article 60(3) GDPR, “*The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views*”;

2. In the present case

14. [REDACTED] is authorised as a Bank in Luxembourg pursuant to the Luxembourg Act of 5 April 1993 on the financial sector, as amended. It is subject to the regulatory framework applicable to banks and supervised by the competent national supervisory authority Commission de Surveillance du Secteur Financier (CSSF). [REDACTED] is also subject to the obligation of professional secrecy set out in Article 41 of the aforementioned Act and shall keep secret all information entrusted to it in the context of its professional activity. The disclosure of such information is punishable, under Article 458 of the Luxembourg Penal Code.
15. Following the intervention of the Luxembourg supervisory authority, the controller informed the CNPD:
 - That the complainant previously encountered difficulties logging into his [REDACTED] account and that his frustration at being unable to solve this problem led to him opening a new [REDACTED] account and requesting the erasure of his old account to start anew.
 - The controller identified that the complainant emailed two different email addresses to request account closure and data erasure in relation to his old account. Also, when the complainant telephoned [REDACTED] to exercise his data

**Deliberation n° 12/RECL7/2025 of 17 January 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 8.843 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 416588**

subject rights, he was unable to authenticate his identity as he could not recall sufficient data points to prove to the controller that he was the account holder.

- Eventually, the controller has established that the complainant provided photo identification to facilitate authentication of his identity and account closure. The controller has then taken action to close the old account and trigger the beginning of the data retention period, following the expiration of which his data will automatically be deleted.
- The complainant has been informed that the account has been closed. A copy of this communication was sent to the CNPD.

3. Outcome of the case

16. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 GDPR.

17. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint. Moreover, the CNPD is of the view that the issue has been resolved in a satisfactory manner.

18. The CNPD then consulted the supervisory authority of Brandenburg (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Brandenburg (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 8.843 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority. As per Article 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller.



**Deliberation n° 12/RECL7/2025 of 17 January 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 8.843 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 416588**

Belvaux, dated 17 January 2025

The National Data Protection Commission

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



DECISION

OF

THE COMMISSION FOR PERSONAL DATA PROTECTION

REF. NO. ПАИКД-13-40/2022

SOFIA,

The Commission for Personal Data Protection (CPDP, the Commission), composed of: Chairman: [REDACTED] and Members: [REDACTED] and [REDACTED], at a meeting held on 13 september 2023, examined and discussed a file with ref. No. ПАИКД -13-40/14.07.2022. In pursuance of a decision of the CPDP from a meeting held on 7 September 2022, an on-site inspection was carried out due to the existence of a “high level of risk” for the rights and freedoms of natural persons. The inspection was related to a received Notification with ref. No. ПАИКД -13-40/14.07.2022 of a personal data breach under Article 33 of Regulation (EU) 2016/679, submitted by SIBERIAN WOLF EOOD (the Controller, the Company). The results of the inspection are objectified in the Report of findings with ref. No. ППН-02-439/06.07.2023.

I. The following factual situation has been established:

The Commission for Personal Data Protection has been approached with a notification of personal data breach under Article 33 of Regulation (EU) 2016/679 (“the GDPR”, “the Regulation”) with ref. No. ПАИКД-13-40/14.07.2022 from SIBERIAN WOLF EOOD and a supplementary letter with ref. No. ПАИКД -13-40#3/10.08.2022, in which the facts of the breach were presented.

SIBERIAN WOLF EOOD have notified the supervisory authority that in connection with the implementation of its commercial activity related to virtual currencies, the company assigned to [REDACTED] and [REDACTED] the development of a website: www.wolfintech.com, through which the company’s customers would be able to use the services it offers in relation to virtual currencies and crypto-asset entrustment.

The company has stated that they did not enter into a written contract with the natural persons who developed the website that would regulate their relationship. The work was assigned on the basis of oral agreements between the parties, under the conditions of good faith cooperation and collegiality in relationships.

After the development and launch of the information system and providing the company’s customers with access to make registration accounts in order to use the company’s



services, the controller requested from the persons who developed the website to provide all passwords, codes, keys for access and administration of the website (www.wolfintech.com) and the back-end components. Since the controller did not voluntarily and immediately obtain access and control over the website, due to the disagreement of the persons who developed the website to provide them, the company considers that there is unregulated access by them to all the data of the subjects – customers of the controller.

From the creation of the website in March 2022 until 27 June 2022, SIBERIAN WOLF EOOD, in its capacity as the contracting entity for the elaboration of the website, had no access to the website administration data, passwords, codes, access keys. Despite repeated invitations to [REDACTED] and [REDACTED] to hand over all passwords and access data to the website, the information was not received. The company was not able to use and manage its information system, it had no access to administer, process and store the information data on the website, including contractual information and personal data of the counterparties of SIBERIAN WOLF EOOD, which is contained in the information system www.wolfintech.com.

On 27 June 2022, after repeated requests and efforts by the company and after an official written notification and invitation, [REDACTED] provided a list of data and passwords for accessing the information system, which was not exhaustive. For full access to the resources of the server where the information system is installed, an additional access verification code is required and this code is sent to a telephone number which is alien to the controller at each attempt to access the website. For this reason, it was impossible to use and administer the information system in full, as they were placed in technical impossibility to do so. [REDACTED] provided partial assistance for the controller's ability to access the information system and all the data contained in it. He offered to render additional assistance, provided that he was paid an additional fee other than what he was originally paid for the development of the website.

On 4 July 2022, SIBERIAN WOLF EOOD found that the access code to the content management system of the website (WordPress.com) had been changed by a third party without their consent. This confirms the fact that there had been unregulated access by a third party to an information system (website) and the controller had not yet had full access and control over the system and all the data contained in it.

The company allowed the registration of customers for the use the services provided, as it agreed with the persons who developed the website that they would provide professional and technical assistance until all registrations of the company's customers who had previously expressed a desire to use its services were completed. In order to complete the customer registration process, it was necessary to create accounts by requesting registration on the website, to fill in the "Know Your Customer" questionnaires, as well as the declarations within



the meaning of the Act on the Measures on Anti-Money Laundering (AMAML). Only after performing these actions, technical authorisation of each customer was carried out through the website and the registration on the website was confirmed. Without obtaining this full authorisation, customers would not be able to use the company's services and entrust their intended cryptoassets (bitcoin). For these technical actions on authorisation the company trusted the persons who created the website. This made necessary the registration of customers in the information system before the acquisition of full controller rights by the company.

The company has stated that an internal investigation was carried out in relation to the incident and they did not find any illegal acquisition, storage or distribution of personal data of the customers. **However, in view of the fact that the persons who developed and administered the website had access to all information and data contained and stored on the website and in view of the fact that these persons did not voluntarily provide all passwords and access keys within the specified period, it can be concluded that there is a risk of possible fraudulent use of a large volume of personal data.**

After repeated invitations to the persons who developed the website to hand over to the company all passwords and keys for access and administration of the website and after negotiations with them, as well as with the help of an expert technical (IT) team, the company was able to acquire a full access to the information system and to all stored data of the company's customers, as well as to suspend any possibilities for unlawful interference and access by third parties. The data are currently stored on a secure storage device (in a secure cloud space) and the data transfer is carried out with the help of an expert technical (IT) team.

Number of data subjects affected by the breach – a total of **129 natural persons**.

126 natural persons – citizens of Italy;

1 natural person – citizen of Romania;

1 natural person – citizen of Moldova;

1 natural person – citizen of Bulgaria.

Categories of personal data affected by the breach:

As an obligated person within the meaning of Article 4(38) of the AMAML, SIBERIAN WOLF EOOD collects the data required by law about its counterparties and performs monitoring in compliance with the Internal rules on control and prevention of money laundering and financing of terrorism, adopted by the Company.

The categories of personal data affected by the breach are the following: **names; personal identification number, copy of identity card, place of birth, telephone number; e-mail; origin (racial, ethnic); property status; financial position; origin of assets; a self-**



made photo of a person taken by the subject for the purpose of identifying and proving the subject's identity with the person whose passport data have been provided.

The following technical and organizational measures have been taken:

- The controller has informed all customers and data subjects about the circumstances. It is recommended that all customers download their data from the website, store them on their own media, outside the website and, at their discretion, print them out for storage on paper;
- On a secure medium, with the help of specialists (in a secure cloud space), secure copies of all the data of the subjects who provided them during their voluntary registration on the website are stored;
- Through an external company, the overall control of the information system was restored.

II. Actions undertaken by the CPDP:

1. On the occasion of the notification received, by a letter from the CPDP, ref. No. ПАИКД-13-40#1/29.07.2022, information and relevant documents have been requested from SIBERIAN WOLF EOOD.
 - a. By a letter with ref. No. ПАИКД-13-40#3/10.08.2022 information and additional documents were received by the CPDP.
 - b. By Report note, ref. No. ПАИКД-13-40#4/02.09.2022, the received notification was reported at a meeting of the CPDP held on 7 September 2022 and a Decision was adopted to carry out an on-site inspection due to the presence of a “high level of risk” for the rights and freedoms of natural persons.
 - c. With a view to clarifying facts and circumstances relevant to the case, Order No. РД-15-73/03.03.2023 ordered the performance of on-site inspection of the personal data controller SIBERIAN WOLF EOOD.
 - d. By a letter, ref. No. ПАИКД-13-40#15/17.02.2023, a notification was sent to SIBERIAN WOLF EOOD regarding the upcoming inspection on 7 March 2023.
2. On the basis of Article 56(1) of the GDPR, the CPDP has initiated a procedure as a supervisory authority competent to act as lead supervisory authority for cross-border processing carried out by a controller established in the Republic of Bulgaria. The procedure was initiated by the Commission on 17 December 2022 and is registered



in the Internal Market Information System under number A56ID 437940. After the expiry of the statutory period, no objections were raised by the other concerned supervisory authorities, Italy and Romania, and the decision is therefore final.

III. Carrying out an on-site inspection at the controller's registered office

The inspection was opened on 7 March 2023 at the registered office of SIBERIAN WOLF EOOD, located in the city of Sofia, Mladost 3, 51 Aleksandar Malinov Blvd., Metro City Shopping Centre, Office No. G 21. [REDACTED], a citizen of the Republic of Italy, manager of the company, was served with the inspection order, in the presence of [REDACTED] – a lawyer from the SBA ([REDACTED]) and [REDACTED] - a translator, who provided assistance and ensured access and collection of evidence by the inspection team.

The tasks of the inspection were clarified and the data and circumstances regarding the incident were discussed. The actions taken by SIBERIAN WOLF EOOD in relation to the personal data breach were discussed.

- The company does not have specifically developed rules and criteria to apply when selecting service providers to develop the website. The persons who were selected assured the manager of their professional qualities, technical skills and knowledge for the purposes for which they were engaged. They gave an assurance that they would take care of the creation of the information system, the preparation and publication of a Privacy Policy and Cookie Policy that are suitable for the website, the secure storage of provided data and the successful commissioning and operation of the website.
- During the design and development of the website, as well as after its commissioning until the establishment of the circumstance – subject of the specific personal data breach notification, the company did not have any access to the website administration data, passwords, codes, access keys. During the entire period from the creation of the website until 27 June 2022, only [REDACTED] and [REDACTED] had access to the www.wolfintech.com information system.
- The company had a verbal agreement with the persons who developed the website that they would provide professional and technical assistance until all the registrations of the company's customers, who previously expressed a desire to use its services, were completed. Before the incident was established, the company fully entrusted the design and development of the website www.wolfintech.com to the persons [REDACTED] and [REDACTED] including the provision of the appropriate technical protection of the website, as well as the preparation and publication of appropriate Privacy Policy and Cookie Policy on the website.



The company has stated that they repeatedly invited [REDACTED] and [REDACTED] to hand over immediately all passwords and access data to the website. In practice, the controller SIBERIAN WOLF EOOD was in no way able to use and manage its own information system www.wolfintech.com. It had no access to administer, process and store information data on the website, including contractual information and personal data of counterparties/customers of SIBERIAN WOLF EOOD. The company was unable to carry out freely and unimpededly its commercial activity, store and lawfully process contractual information and data of its counterparties, which they voluntarily provided in relation to the registration and creation of their accounts on the website www.wolfintech.com for the purpose of using the services provided by the company.

SIBERIAN WOLF EOOD specifies that potential citizens affected by the security breach are: **citizens of Italy – 126 natural persons; citizens of Romania – 1 natural person; citizens of Moldova – 1 natural person and citizens of Bulgaria - 1 natural person.**

The company has appealed for assistance to the hosting platform www.infomaniak.com, being the web hosting of www.wolfintech.com and to the information system www.sectigo.com, which in turn takes care of the cyber security of www.wolfintech.com, but until 14 July 2022 they did not obtain the necessary timely assistance.

SIBERIAN WOLF EOOD has stated that on 27 June 2022, after repeated requests and efforts, [REDACTED] sent a list of data and passwords for access to the information system www.wolfintech.com, which is not exhaustive. For full access to the resources of the server where the information system is installed, an additional access verification code is required and this code is sent to another's telephone number at each attempt to access the website. Thus, it was impossible for the company to use and administer the information system in full. [REDACTED] rendered partial assistance in providing full access to the information system and all the data contained in it. He made it a condition that for the provision of full assistance he had to be paid additional remuneration.

On 4 July 2022, it was found that the access code to the content management system WordPress.com had been changed by a third party, without the consent of SIBERIAN WOLF EOOD. For this reason, the company still did not have full access and control over the information system and all the data contained in it. In this regard and in view of the above, the manager of SIBERIAN WOLF EOOD – [REDACTED] filed a complaint with the Sofia Regional Prosecutor's Office (ref. No. 28966/14.07.2022). Subsequently, they were informed that the file was terminated and a refusal to initiate pre-trial proceedings was ruled.



During the entire period from the creation of the website until 14 July 2022, access to the company's information system www.wolfintech.com was available only to [REDACTED] and [REDACTED]. It was also found by the company that at the end of June 2022, changes were repeatedly made to the website, information data were deleted, new information was added, the access of the company's registered counterparties to the information contained in their existing accounts at www.wolfintech.com was restricted and it has not been established who committed these illegal acts – without the consent of the company and without the consent of the counterparties registered on the website.

In order to carry out its commercial activity and to fulfil its contractual commitments to its counterparties, the company aimed to use entirely the website www.wolfintech.com. **The lack of access to control, storage and management of the information data on the website put the company in a complete inability to fulfil its obligations to its counterparties and completely hindered the lawful processing and storage of the provided personal data.**

[REDACTED] has stated that according to the information that he was provided with by [REDACTED] and [REDACTED] at the stage of design and construction of the information system www.wolfintech.com, the system was protected by an anti-virus program, passwords and access codes, which were available only to the persons entrusted with the creation of the website – [REDACTED] and [REDACTED]. **The company has no specific documents regarding this circumstance.**

After the occurrence of the incident and in view of protecting the interests of customers and protecting the data provided by them upon registration, SIBERIAN WOLF EOOD commissioned to the specialised company Bcademy Sri. (address Via Piave 26. Pordenone 33170, Italy, VAT number 01838830931) to carry out a complete audit of the information system, to obtain all access codes and to prevent any possibility of a third party's access to the system. The expert technical team of the company Bcademy Sri. performed a comprehensive audit of the information system www.wolfintech.com, for which a Forensic Analysis Report on the website www.wolfintech.com was drawn up on 22 July 2022. After an automatic and manual analysis of the website's code from backup copies made on different dates, it was concluded that www.wolfintech.com did not contain any malicious code in its content.

After an additional inspection and assessment of the condition of the assets of www.wolfintech.com, which was assigned by SIBERIAN WOLF EOOD, a report was drawn up by Dracteam Technology LLC on 7 November 2022 and the following was done:

- Full ongoing scanning for malware detection;
- Scanning files on websites for integrity control;
- Checking the latest PHP version;



- Checking the integrity of the SQL DB (the database);
- Checking folder permissions;
- Latest version of the Content Management System (CMS);
- Checking for access and modification of critical data of the original/child website template;
- Checking the latest version of plugin (a software component that adds a specific function to an existing computer program);
- Checking the consistency and compatibility of the plugin;
- Verification of the authentication management process;
- Checking the validity of the SSL (cryptographic protocol for client-server connection) server;
- Third-party software verification www.passbase.com;
- Know Your Customer (“KYC”) software;
- Comprehensive website diagnostics and performance.

The report outlined the following results of the inspection of www.wolfintech.com:

- No traces of malicious code were found;
- Some of the original files from the template’s child theme were code modified by the previous web administrator to adjust and force the native content CMS workflow;
- The latest process for automatic registration/approval of the user did not comply with the initial request agreed with SIBERIAN WOLF EOOD;
- User login/registration workflow was not designed properly;
- The workflow designed to complete automatically the contract was not fully automatic and was not directly related to KYC.

In relation to the identified problems and after coordination with SIBERIAN WOLF EOOD, the following actions were taken:

- Re-changing any pre-existing access credentials;
- Moving outside of the actual website any link related to the Application Programming Interface (“API”) at www.passbase.com;
- Reducing the field of sensitive data in the user registration form as a temporary collection of potential customers (if necessary): “first name, last name, country of origin, e-mail ID (identifier)”;
- Creating a brand new Privacy Policy and Cookie Policy with pre-emptive blocking and asynchronous reactivation regarding the new upcoming website project in accordance with digital laws and regulations;



- Changing the status of www.wolfintech.com to “Under Maintenance” for security and protection of user data.

During the inspection, gaps were identified that were related to the lack of clear criteria and rules for selection of a contractor for the development of the company’s initial information platform www.wolfintech.com. No written contract was concluded to regulate clearly and in detail the relations between the company and the natural persons who developed the website www.wolfintech.com – [REDACTED] and [REDACTED] and to regulate how and at what stage the company would have full access to its website, as well as the liability and penalties for non-performance on behalf of the contractor.

The controller has announced that, following the expert forensic analysis of the website, it was found that the persons who created the website had access only to the information which was stored on the website and that the personal data that were contained on the platform were the name and e-mail of the relevant subject – customer of the company. All other data, such as passport data, address, place of birth, telephone number, were stored in the company’s account, again in the information platform www.passbase.com, and only the manager – [REDACTED] – had access to this account. **But the forensic report provided by Dracteam Technology LLC did not conclusively confirm this fact. Therefore, the controller’s claims regarding the said circumstance are unproven.**

Following the incident, the website www.wolfintech.com was suspended and the company took steps to develop a completely new information platform in order to continue providing its services to customers.

When planning the inspection, the inspection team was informed that all activities and functionality on the old website www.wolfintech.com are suspended and for the purposes of the services offered by SIBERIAN WOLF EOOD, a new information system www.siberianwolf.biz is being developed. The purpose of using the platform is to inform customers about the services provided by the company. If interested, the customer can fill in a contact form to get more information.

Currently, the company has adopted the following policies, rules and procedures for personal data protection:

- Internal rules for personal data protection;
- Procedure concerning personal data security breach;
- Register of personal data security breaches;
- Risk assessment standard in the processing of personal data;
- Privacy policy of the company’s showcase website www.siberianwolf.biz;



- Cookie policy of the company's showcase website www.siberianwolf.biz.

During the inspection, [REDACTED] demonstrated the functionalities of the current website www.siberianwolf.biz. It has been established that personal data are processed on two information platforms whose services are used by SIBERIAN WOLF EOOD and to which the company has commissioned data processing. Any natural person who wishes to familiarise himself/herself with the services provided by the company should visit the showcase website www.siberianwolf.biz and choose whether to continue using the website, having previously familiarised himself/herself with the published Cookie Policy and declaring his/her agreement that he/she is familiar with the relevant Cookie Policy and that he/she wishes to continue using the website. In the event that the natural person wishes to receive more information about the services provided by the company or to declare his/her intention to use the services offered by SIBERIAN WOLF EOOD, the customer has the opportunity by using the contact form to send an inquiry to the company. The website contains a contact form with the company and for this purpose SIBERIAN WOLF EOOD uses the services of a third party – a service provider that allows website owners to add personalised contact forms to their websites. In this case, the natural person should declare that he/she has familiarised himself/herself with and accepts the Privacy Policy published on the website, and that he/she voluntarily provides his/her personal data – name and contact e-mail, and agrees for these data to be processed in accordance with the accepted conditions of the Privacy Policy published at www.siberianwolf.biz.

For the purposes of the company's activity, the services of a third party that is external to the company were used – a service provider – for creation and integration of personalised contact forms to websites. For this purpose, the company, as a website owner, uses an external service at www.iotform.com for the creation and management of contact forms.

The controller uses the services of the international platform Passbase Inc., which is a set of identification tools, including vitality detection, document verification, face recognition, etc. These tools are combined to assess the authenticity of a user's true identity. Passbase Inc. provides the ability to verify securely users from over 190 countries without having to store their data. User submits a video selfie and valid identification resources during verification. Once all the necessary resources are provided, the data points are extracted, digitized and authenticated. These data points then become part of the user's identity. User is required to provide consent to share resources and/or data points of their identity. This information is transmitted and can be used to make decisions about the user (e.g. account activation).

All data of natural persons – customers of the company, are collected, processed and stored by the platform www.iotform.com and by the platform www.passbase.com. The www.passbase.com platform has built its system in compliance with the California Consumer



Protection Act (CCPA) to ensure a high level of privacy and in compliance with Regulation (EU) 2016/679.

SIBERIAN WOLF EOOD, as a user of the platform www.passbase.com and the services provided by it, has access to an account with data of the natural persons – customers of the company. Only the company manager has passwords and access codes to the company's account on the www.passbase.com platform. Passwords and access codes are stored on paper, sealed in an envelope and located in the company's safe in a Bulgarian commercial bank. Only [REDACTED] – manager of SIBERIAN WOLF EOOD has access to the safe. The company's access is limited to the extent that the manager can familiarise himself with the data provided by a natural person – a potential customer of SIBERIAN WOLF EOOD, in order to assess the risk profile of the customer, according to the AMAML, and to assess whether the customer agrees to use company services. The manager of SIBERIAN WOLF EOOD has no ability to copy, download, store, delete or correct customer data.

In relation to the operation of the new website www.siberianwolf.biz, the company assigned the preparation of a Compliance Report made by an expert team of Dracteam Technology LLC, in which no inconsistencies are reported regarding the personal data processed and regarding the security measures taken.

On 1 March 2022, the company adopted the Risk Assessment Standard in the personal data processing of SIBERIAN WOLF EOOD. The need for a data protection impact assessment at the start of each project is identified, assessing the project and the type of personal data associated with it or the processing activity. Proceeding from the initial arrangements with the contractors [REDACTED] and [REDACTED] for the creation of an information system www.wolfintech.com and considering the fact that the data should have been collected under the conditions of the availability of control possibilities, guaranteed rights of the subjects, implemented monitoring and reporting mechanisms, data structuring, anonymisation, encryption or pseudonymisation mechanisms at the time of assignment and development of the previous website. **The controller has reports that the risk was determined to be low, without providing evidence of a risk assessment, impact assessment or other analysis, based on which the provision of the company's customer data was allowed through www.wolfintech.com to third parties without written documents and security guarantees.**

Until now, the company has not received any alerts, complaints or other form of information from natural persons regarding illegal processing of their personal data or misuse thereof as a result of the incident.



All data subjects were informed of the fact that the persons who developed the previous information platform of the company – www.wolftntech.com, affected by the incident, had access to the data therein. The manager of the company sent a written notification to the persons who developed the website and a warning that they have to provide him with all passwords for access and control over the website, as well as to suspend their access to the website and the data stored in it. The data subjects were notified by electronic correspondence in an official group created by means of the communication and instant messaging application Telegram, this group being created for the purpose of direct and rapid communication with all customers of the company (data subjects) and group participants. The data subjects were also informed through telephone conversations and during a virtual video conference through the Zoom video communication platform, which was transmitted live between all participants.

IV. Conclusions of the inspection:

On the basis of the findings of the inspection, which are recorded in the Report of Findings with ref. No. ППН-02-439/06.07.2023, it is established that SIBERIAN WOLF EOOD, in its capacity of “Data Controller” within the meaning of Article 4(7) of the GDPR, has committed a data security breach when carrying out its activity, namely: it has lost control over the personal data that are collected and processed on its behalf – the persons who developed the website (www.wolftntech.com) had full control over them, including the personal data contained therein, without the controller’s consent. **The personal data breach described in notification with ref. No. ПАИКД-13-40/14.07.2022 is evident of the fact that SIBERIAN WOLF EOOD did not take technical and organisational measures to ensure an appropriate level of security of the personal data provided by the controller’s customers.** The company should have implemented measures that comply in particular with data protection principles “Privacy by design and by default”. When determining which measures are appropriate, the controller should assess the current technical and technological achievements in combination with the costs of implementation, the nature, scope, context and purposes of the processing, as well as the risks of varying probability and severity to the rights and freedoms of natural persons. After carrying out such assessment and analysis, SIBERIAN WOLF EOOD should have implemented appropriate technical and organisational measures to ensure a level of security consistent with the specific risks. This is enshrined in the obligation envisaged in the provision of Article 25 of the GDPR, which refers to “Privacy by design and by default”. The fulfilment of this obligation, as well as the obligation to introduce appropriate technical and organisational measures, according to Article 32(1) of the GDPR are conditions that guarantee compliance with the principle of integrity and confidentiality (Article 5(1)(f) of the GDPR).



The responsibility of SIBERIAN WOLF EOOD is, according to Article 5(2) of the GDPR (principle of accountability), to demonstrate compliance with the data processing principles defined in Article 5(1) of the GDPR. In this regard, the controller should properly document all processes of personal data processing. It is necessary to create a documentary environment regarding the personal data processing – to have written documents that allow traceability of data processing processes. Thus, it can be proved that the data is processed lawfully, in good faith, transparently and in a minimum volume to achieve the clearly defined objectives, and the data is stored accurately and only for the time necessary to achieve these objectives, and the said processing is ensured with an appropriate level of security and data protection. **In the specific case, the controller did not take these actions, therefore it is unable to prove compliance with Article 5(2) of the GDPR (“accountability”).**

Also, when a controller uses the services of a personal data processor for the processing of personal data, the provisions of Article 28 of the GDPR should be observed, namely: SIBERIAN WOLF EOOD should use a processor that provides sufficient guarantees for the application of appropriate technical and organisational measures. The relations with the processor should be regulated by a contract or other legal act (made in writing), which is binding and regulates the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and the rights of the processor and of the controller. It is evident from the performed inspection that SIBERIAN WOLF EOOD, in its capacity as a Data Controller, did not take any actions for the processing to proceed in accordance with the requirements of the GDPR and is not able to prove compliance with the requirements of Article 28 of the GDPR.

The controller allowed the development and implementation of technical security measures to be made by persons with whom it did not have a contract specifying what technical and organisational measures should be taken when developing and implementing the website – www.wolfintech.com. In relation to its activity, the controller should have collected and processed a large volume of personal data of its customers, including those, the access to which may cause serious financial losses for the data subjects. The company has not assessed the risks of varying probability and severity for the rights and freedoms of natural persons. Given the fact that there were no clear rules and criteria regarding the technical and organisational measures upon the development of the website, the controller allowed the persons who developed it to have uncontrolled access to the provided data, being unable in this period to ensure the relevant security and guarantees for the lawful processing of the data provided by the customers. This has also been confirmed by Dracteam Technology LLC, which carried out an inspection and assessment of the assets of www.wolfintech.com.



For the purposes of the services offered by SIBERIAN WOLF EOOD, a new information system www.siberianwolf.biz was developed.

V. Legal analysis

General Data Protection Regulation, which applies from 25 May 2018, is the legal act defining the rules related to the protection of the personal data of natural persons during their processing. The GDPR builds on the previous data protection regime introduced by Directive 95/46/EC, transposed into the Bulgarian Personal Data Protection Act of 2002, while at the same time taking into account the dynamics of the development of new technologies and of personal data processing activities.

According to the legal definition referred to in Article 4(12) of the GDPR, “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. In this particular case, third parties had access to the data sets of the controller and an opportunity to acquire them without hindrance. Due to the fact that the controller did not take the necessary technical and organisational measures, the third parties had access to data on 129 natural persons – data subjects. The combination of personal data to which the third parties had access allowed easy identification of the affected data subjects, without the need for additional efforts:

- Basic data – names; personal identification number, copy of identity card, place of birth, telephone, e-mail, photo of the person for the purpose of identification and proof of identity with the subject whose passport data are provided;
- Sensitive data – racial, ethnic origin;
- Financial data – property status, financial status, origin of assets.

After the entry into force of the GDPR on 25 May 2018, personal data controllers have an obligation to maintain the security of personal data in a way that prevents processing in breach of the Regulation. It should be noted that Article 24 of the GDPR introduces an **obligation and responsibility** for the Data Controller to implement the appropriate technical and organisational measures, taking into account the factors listed in the same Article. **In this regard, the controller should carry out an assessment of the risks associated with the specific processing and take measures to limit these risks.** The measures must ensure an appropriate level of security, including confidentiality, taking into account the state of technical progress and the costs of implementation in relation to the risks and the nature of the personal data to be protected. The data security risk assessment implies consideration of the specific risks arising from the processing of personal data by the particular controller – such as accidental or unlawful destruction, loss, alteration, unlawful disclosure, or access to



transmitted, stored or otherwise processed personal data. It should be assessed whether the risks described in the previous sentence that are related to the processing of personal data may lead to physical, material or non-material damages. This means that the controller must, in addition to processing only the personal data necessary for the performance of its functions, have also implemented strict mechanisms that make it possible for it to exercise increased control over the data and prevent unauthorised access and distribution, as stated in the case. **During the review of the case, it was established that the Data Controller SIBERIAN WOLF EOОD did not perform a risk analysis before the personal data breach.** As a consequence of the stated circumstance, the controller SIBERIAN WOLF EOОD did not comply with the principles of “privacy by design” and of “privacy by default”, in accordance with the provisions of Article 25 of the GDPR, accordingly, it did not take appropriate technical and organisational measures and this led to the occurrence of the incident under consideration. In relation to the above, the controller violated **Article 5(1)(f) in conjunction with Article 32(1)(d) of the GDPR – by failing to perform an analysis and assessment of the effectiveness of the technical and organisational measures in order to ensure security of processing.**

One of the primary duties of data controllers is accountability. It is enshrined in the specific principle formulated in Article 5(2) of the GDPR and it assigns to them the responsibility to document their personal data processing actions and achieve compliance with the principles of personal data protection. It is expressed in the controller’s obligation to maintain documentation in relation to the personal data it processes, describing on what legal basis it processes the data, for what period of time, as well as to prepare and implement specific privacy policies and other relevant documents. **In this particular case, at the time of the occurrence of the incident, the controller did not have written internal rules for the processing of personal data related to the specific subject matter of activity of SIBERIAN WOLF EOОD. With regard to the above, the controller does not prove any compliance with Article 5(1) of the GDPR and thus a breach of the “principle of accountability” under Article 5(2) of the GDPR has been committed.**

Article 28 of the GDPR imposes an obligation on the respective controller to use only personal data processors which provide sufficient guarantees for the application of appropriate technical and organisational measures in such a way that the processing takes place in accordance with the requirements of the GDPR and ensures sufficient protection of the data subjects’ rights, such as reliability and resources, that they will take technical and organisational measures that meet the requirements of the GDPR, including the requirements for security of processing. The performance of processing by a personal data processor should be regulated in writing between the controller and the processor with a contract or other legal act. The document



should regulate the subject matter and the duration of the processing, the nature and purposes of the processing, the type of personal data and the categories of data subjects, taking into account the specific tasks and responsibilities of the personal data processor in the context of the processing to be carried out, as well as the risk to the rights and freedoms of the data subject. The written document between the controller and the processor should contain clauses according to which, after the completion of the processing on behalf of the controller, the personal data processor must hand over the relevant documents. **It follows from the above that SIBERIAN WOLF EOOD did not comply with the provisions of Article 28 of the GDPR, having assigned through a verbal agreement and in the absence of clear criteria for selection of a contractor to develop the company's website www.wolfinetech.com. No written contract has been concluded that clearly and in detail regulates the relationship between the company and the contractors who developed the website www.wolftntech.com, and regulates how and at what stage the company will have full access to its website. The responsibility and sanctions against the developers of the website www.wolftntech.com in case of non-fulfilment, including with regard to the legality of the actions related to the processed personal data, have not also been agreed upon.**

The CPDP has operational independence and, in accordance with the functions assigned to it, it makes an assessment as to which of its corrective powers under Article 58(2) of the GDPR to exercise. The assessment is based on considerations of expediency and effectiveness of the decision, taking into account the particularities of each specific case and the degree of impact on the interests of the specific natural persons – data subjects, as well as the public interest. The powers under Article 58(2) of the GDPR, without those under (i), have the nature of coercive administrative measures, the purpose of which is to prevent or stop the commission of a violation, thus achieving due behaviour in the field of personal data protection. The administrative fines under Article 58(2)(i) of the GDPR have a punitive nature.

In applying the appropriate corrective measure under Article 58(2) of the GDPR, the nature, gravity and consequences of the infringement, as well as any mitigating and aggravating circumstances, shall be taken into account. The assessment of what measures are effective, proportionate and dissuasive in each individual case also reflects the objective pursued by the selected corrective measure – prevention or termination of the infringement, sanctioning of illegal behaviour or both and such possibility is provided for in Article 58(2)(i) of the GDPR.

According to Article 83(2) of the GDPR, depending on the circumstances in each specific case, the administrative fines are imposed in addition to the measures under Article 58(2) of the GDPR. When imposing an administrative fine under Article 58(2)(i), of the GDPR



and determining its amount, an analysis of the elements in Article 83(2)(a) to (k) of the GDPR should be duly made in each specific case.

In this particular case, the analysis is as follows:

- a) Affected data regarding: names; personal identification number; a copy of an identity card; place of birth; telephone; e-mail; a photo of the person for the purpose of identification and proof of identity with the subject whose passport data are provided; sensitive data – racial, ethnic origin; financial data – property status, financial status, origin of assets. By means of the listed data, the persons can be unambiguously identified, respectively, the potential impact on the data subjects can lead to a loss of control over their personal data, as well as a loss of privacy of the personal data of the affected subjects;
- b) In this particular case, the violation was committed intentionally. The fact that the controller did not take sufficient appropriate technical and organisational measures to preserve the confidentiality of personal data contributed to a large extent to the commission of the violation;
- c) The controller SIBERIAN WOLF EOOD sent several invitations to [REDACTED] and [REDACTED] to hand over all passwords and access data to the website, but no information was received. The controller was not able to use and manage its information system, it did not have access to administer, process and store the information data on the website, including contractual information and personal data of the customers of SIBERIAN WOLF EOOD, contained in the information system www.wolfintech.com;
- d) In this particular case, the Data Controller is fully responsible for the occurrence of the personal data breach, since it did not take appropriate technical and organisational measures to protect the confidentiality of the personal data as early as at the stage of design (it did not carry out a risk assessment in accordance with the main criteria laid down in the GDPR; at the time of the violation, the controller did not have internal rules regulating the lawful processing of personal data; did not select personal data processors that provide sufficient guarantees for the implementation of appropriate technical and organisational measures in such a way that the processing takes place in accordance with the requirements of the GDPR and ensures sufficient protection of the rights of the data subjects; did not enter into a written contract with the processors, having the minimum required content specified in Article 28(3)(a) to (h) of the GDPR);



- e) In this particular case, with respect to the controller, there are no related previous violations of a similar nature;
- f) The personal data controller has cooperated with the CPDP in order to eliminate the violation and mitigate its possible adverse consequences;
- g) The violation has affected the following categories of personal data: names; personal identification number; a copy of an identity card; place of birth; telephone; e-mail; a photo of the person for the purpose of identification and proof of identity with the subject whose passport data are provided; sensitive data – racial, ethnic origin; financial data – property status, financial status, origin of assets. Through these data, the affected data subjects can be fully identified;
- h) The personal data breach became known to CPDP directly from the Data Controller;
- i) No previous corrective measures have been imposed on the controller;
- j) In view of the fact that there is not yet an approved code of conduct in the Republic of Bulgaria, according to Article 40 of the GDPR, the controller does not adhere to such a code;
- k) The non-application of technical and organisational measures by the controller, which allowed the occurrence of the incident under consideration, should be taken into account as an aggravating factor. The controller's cooperation with the CPDP and the fact that the controller notified the persons affected by the violation should be taken into account as mitigating factors.

In this particular case, only the issuance of an order and the imposition of a corrective measure under Article 58(2)(d) of the GDPR is not enough. According to the reasons described above and taking into consideration the nature and type of the found violation, it is expedient, proportionate and dissuasive to impose a measure under Article 58(2)(i) of the GDPR, namely imposition of a fine on the controller SIBERIAN WOLF EOOD. After the accomplished analysis and evaluation of the evidence gathered in the case and taking into account the extenuating circumstances, the Commission for Personal Data Protection considers that the imposed specific measure will have a warning and deterrent effect and will contribute to the compliance with the established legal order on behalf of the controller.

In view of the above, after review and analysis of all evidence gathered in the administrative file, in order to prevent future similar violations, the Commission for Personal Data Protection has adopted the following



DECISION:

1. Pursuant to Article 58(2)(d) of the GDPR for violation of Article 5(1)(f) in conjunction with Article 32(1)(b) and (d) and Article 5(2) of the GDPR, it **ORDERS** for the Data Controller SIBERIAN WOLF EOOD:

- To provide for performance of periodic risk analysis in its internal documents (determining a specific period in which it should be performed), and in the case of the introduction of new technology, it should be mandatory;
- To provide for compliance with the principles of accountability in its internal documents.

The order under item 1. must be executed **within three (3) months of the entry into force of the decision**, and then, within fourteen (14) days, the controller must notify the Commission for Personal Data Protection of its execution, by presenting relevant evidence.

2. Pursuant to Article 58(2)(i) of the GDPR, it imposes on the Data Controller SIBERIAN WOLF EOOD an administrative penalty – **FINE** in the amount of **BGN 10,000 (ten thousand)**, according to Article 83(4)(a) of the GDPR for violation of Article 25, Article 28, Article 32(1)(b) and (d) of the GDPR and Article 83(5)(a) of the GDPR for violation of Article 5(2) of the GDPR.

When determining the appropriate amount of the fine, it is important to note that the GDPR specifies only the maximum amount and the criteria for determining the corresponding administrative fines. The specific amounts should be determined by the supervisory authority on a case-by-case basis, taking into account all the circumstances related to the situation under consideration. According to Article 83(4) and (5) of the GDPR, the maximum amount of the fine shall be up to EUR 10,000,000 or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4), respectively up to EUR 20,000 000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(5)). In this case, given the fact that the controller is a company registered under the Commercial Act, it is obliged on the grounds of Article 38 of the Accountancy Act to announce its Annual Financial Report for the financial year 2022 until 30 September 2023. In this regard, as at the date of the CPDP's meeting – 13 September 2023, at which this decision was taken, the Annual Financial Report of SIBERIAN WOLF EOOD for the financial year 2022 was not yet announced in the Commercial Register. On this occasion, the CPDP has determined a specific amount of the fine, which tends to a minimum amount – BGN 10,000 (ten thousand), which is approximately equal to EUR 5,000 (five thousand), referring to reasons listed in detail and



recorded in the legal analysis of the decision. In addition, the CPDP also takes into account the fact that the company was founded in 2021 and falls into the category of “micro enterprises” within the meaning of the Small and Medium Enterprises Act.

After the entry into force of this decision, the amount of the imposed administrative fine should be transferred by bank transfer to the Commission for Personal Data Protection, Sofia, 2 Prof. Tsvetan Lazarov Str.:

Commission for Personal Data Protection, Bulstat 130961721,

Bank account IBAN: BG18BNBG96613000158601 BIC BNBGBGSD

BNB Bank – Central Office.

In the event that the obligation is not paid voluntarily within the statutory period after the entry into force of the decision, actions will be taken for forced collection, according to Bulgarian legislation.

The decision of the Commission for Personal Data Protection may be appealed to the Administrative Court - Sofia City within fourteen (14) days from its receipt.

The decision was taken at a meeting of the Commission for Personal Data Protection, held on 13 September 2023.

Summary Final Decision Art 60

IMI Number 588536 - Notification

EDPBI:BG:OSS:D:2023: 1066

Administrative fine ; Compliance order; Violation identified

Date of summary: 08/07/2024

Background information

Date of complaint:	N/A
Draft decision:	N/A
Revised draft decision:	N/A
Date of final decision:	13 September 2023
Date of broadcast:	12 December 2023
Controller:	Siberian Wolf EOOD
Processor:	N/A
LSA:	BG
CSAs:	IT SA; RO SA
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 32 (Security of processing), Article 28 (Processor), Article 25 (Data protection by design and by default)
Decision:	Administrative fine, Compliance order, Violation identified
Key words:	Administrative fine, Accountability, Data protection by design and by default, Personal data breach, Responsibility of the controller

Summary of the Decision

Origin of the case

The LSA had been notified of a data breach by the controller whose main activity is acting as an intermediary in the financial sector. The controller had engaged two developers to build a website through which its customers would be able to use the services it offers in relation to virtual currencies. The company had however never entered in a written contract with the developers but rather relied on an oral agreement. After the development and launch of the information system and providing the company's customers with access to make registration accounts, the controller requested the website developers to provide all passwords, codes, keys for access and administration of the website, as well as the back-end components.

Despite repeated invitations, for a number of months, the developers refused to hand over the access codes and passwords to the controller, during which time users could register. Due to these circumstances, the controller considered that there was unregulated access by the developers to all of the controller's customers' personal data for the period between May and June 2022, when the developers partially complied with the controller's request. However, soon after that, the controller found that a third party had changed the codes to access the content management system of the website without the controller's consent. The company allowed the registration of customers to use the services provided, as it agreed with the developers that they would provide professional and technical assistance until all customers registrations who had previously expressed an interest in using its services were completed. Following the incident, the controller commissioned a complete audit of the information system and an internal investigation was carried out. According to the controller, no illicit acquisition, storage or distribution of personal data had taken place and a number of measures were taken in relation to the problems identified, including suspending the website and creating a new information platform.

However, after carrying-out an on-site inspection at the controller's office, the LSA suspected that given the circumstances, there was a risk of possible fraudulent use of a large volume of personal data. A total of 129 data subjects were affected by the breach and the categories of personal data affected were: names, addresses, Personal ID Numbers, copies of ID documents, places of birth, phone numbers, e-mails, origin (racial, ethnic), information related to the individual's property and financial status, origin of assets, photos.

Findings

The LSA considered that the lack of access to control, storage and management of the information data on the website put the controller in a complete inability to fulfil its obligations to its counterparties and completely hindered the lawful processing and storage of the provided personal data. The LSA also found that the controller had not taken appropriate technical and organisational measures to ensure an appropriate level of security of the personal data provided by its customers and hence, did not comply with the principles of data protection by design and by default. In addition, the LSA considered that by not having access to its website, the controller has not complied with the obligation to document the processes of personal data processing and therefore was unable to prove compliance with Article 5(1) and (2) GDPR. Furthermore, the oral agreement does not rise to the rigors of article 28 as firstly, there ought to be a binding contract that governs the controller-processor relation and secondly, aspects such as the purpose and nature of processing, the categories of personal data and the categories of data subjects were never determined.

Decision

The LSA concluded that the controller infringed Article 5(1)(f) in conjunction with Article 32(1)(b) and (d) and Article 5(2) GDPR; ordered the controller to provide, within a period of 3 months, for performance of periodic risk analysis in its internal documents and to ensure compliance with the principles of accountability in its internal documents.

In addition, the LSA imposed on the controller an administrative of 10.000 BGN (approximately 5.000 EUR) for the breach Article 25, Article 28, Article 32(1)(b) and Article 5(2) GDPR.



Berlin, 04 September 2020

535.781
631.91
A56ID 75328
CR 82025
DD 137878
FD 148217

Berlin Commissioner for
Data Protection and
Freedom of Information

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** Apassionata World GmbH
- **Incident:** Attack on Microsoft Office 365 account of the managing director, phishing mails
- **Date of occurrence:** Unknown
- **Date of acknowledgement of the incident:** 25 March 2019
- **EU/EEA Member States concerned, with the number of data subjects concerned:**
 - o Austria: 8
 - o France: 5
 - o Germany: 207
 - o Hungary: 2
 - o Italy: 1
 - o Poland: 1
 - o Portugal: 1
 - o Romania: 2
- **Category of data subjects:** Customers
- **Category of the data types/data records concerned:** Email addresses
- **Likely consequences of the violation of the protection of personal data:** Misuse to send phishing emails

2. Description of the data breach from a technical-organizational perspective

Unauthorized persons have gained access to a Microsoft Office 365 account and manipulated settings. How the unauthorized persons obtained the access-data could not be clarified. Possibly the cause was the receipt of a phishing e-mail of the same type, which was later sent from the account that was also affected, requesting the user to enter the login data for Office 365.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

The password for the affected account has been reset; the manipulated rules for deleting incoming emails have been removed. In addition, the end devices used were checked. The computers used have (and had at the time of the attack) up-to-date, state-of-the-art virus protection.

Retraining on how to handle e-mails and in particular on the compliance goals of encryption, access control and forwarding control.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

The controller has informed all data subjects concerned without undue delay in written form (German, English and French).

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

See 3.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

The cause may have been the receipt of a phishing e-mail of the same type, which was later sent from the account that was also affected, requesting the user to enter the login data for Office 365. Such attacks could be made considerably more difficult if measures were taken to strengthen user authentication, such as 2-factor authentication. However, since it is not apparent that a particularly high number or special types of personal data were affected, we do not consider a corresponding requirement to be appropriate. Nevertheless, the controller was recommended to use measures for stronger user authentication such as 2-factor authentication.

The other IT security measures, in particular those of the service provider Microsoft, should generally be considered sufficient.

7. Intended measures by the LSA Berlin DPA

7.1 Intended measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

7.2 Intended measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has also not identified any data protection violations beyond Articles 33, 34 GDPR.

To: [REDACTED]
From: CBU2Complaints@dataprotection.ie
(By email)

DPC Ref: C -19-5-362

Re: [REDACTED] v [REDACTED]

30 September 2020

Dear [REDACTED],

This is a final decision of the Data Protection Commission (**DPC**) in relation to your complaint originally lodged on 13 May 2019 against [REDACTED]. As you are already aware, the Berlin Commissioner for Data Protection and Freedom of Information (**BfDI**) investigated your complaint because it was the lead supervisory authority for [REDACTED]. This decision is based on the investigation and information provided to the DPC by the BfDI.

The DPC's role in relation to your complaint

The DPC's initial investigation confirmed that the processing at issue in relation to your complaint was 'cross border' for the purpose of applying the General Data Protection Regulation (**GDPR**). This meant that the DPC's role in relation to your complaint was as a concerned supervisory authority, and that the investigation into your complaint would be conducted by the lead supervisory authority for [REDACTED] the BfDI.

The DPC informed you on 25 June 2019 that the BfDI were the lead supervisory authority competent to investigate your complaint. The DPC forwarded your complaint to the BfDI and provided you with regular updates in relation to your complaint.

Decision of the BfDI dated 24 January 2020

Following the conclusion of the investigation into your complaint by the BfDI and subsequent consultations with the DPC and other supervisory authorities in Europe, a draft decision was issued in relation to your complaint pursuant to Article 60 of GDPR.

The BfDI dismissed your complaint based on its investigation into this matter. The decision and reasoning of the BfDI, to which the DPC had no objection, is enclosed for your information.

Final Decision of the DPC

As the supervisory authority with which the complaint was lodged, the DPC must adopt and issue the final decision based on the investigation of the BfDI that your complaint has been dismissed.

Please note, a procedural change impacting whether or not the BfDI or DPC had responsibility for issuing a final decision led to a short delay in issuing this final decision to you. A copy of this letter and final decision will also be provided to [REDACTED] for its information.

Your right to an effective judicial remedy

Article 78 GDPR entitles you to an effective judicial remedy against a legally binding decision of a supervisory authority. The adoption of this dismissal of your complaint is a “legally binding decision” of the DPC as defined in Section 150 (12) DPA. Pursuant to section 150 (5) DPA, you may, within 28 days from the date you received this notice from the DPC, appeal against this decision to either the Circuit Court or the High Court. In the event you are dissatisfied with the final decision and you wish to take the matter further in Ireland or Germany, we suggest getting your own independent legal advice.

Next Steps

As the BfDI have completed its investigation into this matter and the DPC has issued you with the final decision and informed of your rights, the DPC will close its file in relation to your complaint.

Yours sincerely,



Deputy Commissioner

Data Protection Commission



Draft Decision
521.11522
IMI A56ID 71254

Berlin, 24. January 2020

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

The Complaint:

The complainant criticizes that his [REDACTED] app requests the permission to access "location services". The app manufacturer states that this is a requirement of Android 6.0 or higher to be able to scan for Bluetooth LE devices in order to connect to the [REDACTED]. Location data is not used by the app at all.

Our Evaluation:

The statement is (unfortunately) correct, because so-called beacons (for indoor localization) also use Bluetooth. This is a technical restriction of the Android operating system. The procedure is necessary to provide the requested service.

Proposed Action:

The app manufacturer has not breached data protection laws as far as the complaint is concerned. The case should therefore be closed.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>



Ref. 11.17.001.007.263

27 July 2020

BY EMAIL

Data Protection Officer
F1 Markets Limited
Kolonakiou Avenue 43
Diamond Court, Office No: 2B
4103 Limassol, Cyprus

Dear Madam,

Subject: Investigation of complaint under the GDPR - access request of Mr. █ Decision

Further to the exchange of communications between the Office of the Commissioner for Personal Data Protection (the Commissioner) and F1 Markets Limited (the controller) concerning a complaint involving your company, we would like to bring to your attention the following assessment of the Commissioner.

Summary of the Case

On 7 August 2019, Mr. █ sent an email to info@investous.com requesting the closure of his account and access to his data on the basis of article 15 of the GDPR. The email was also sent to his account manager. According to the complaint, the controller did not respond to the access request and the data subject lodged a complaint with the data protection authority in September 2019.

Investigation by the Commissioner

Further to our exchange of communications, you explained that on 17 July 2019, Mr. █ requested from the Customer Support team, account closure and refund of his account, a request which was handled by the Customer Support team. On 18 July 2019, the said team replied to Mr. █ providing specific instructions on how to withdraw the remaining amount from his account in order to be able to proceed with the account closure.

Further to your internal investigation it was found that the email sent by Mr. █ on the 7 August 2019, by which he requested access to his data, was never received as it was quarantined by the email security service and categorized as spam due to the applied information security IT measures for emails received from outside the Company. The account manager who also received the email assumed that it had an informative character and was under processing, since the established procedure for an account closure request is to be forwarded only to the team designated for this role i.e. the Customer Support team. The account manager only confirmed that the Customer Support team was working on the request filed from Mr. █.

As remedial actions to the above malfunctions, you affirmed that you are working with the IT department in order to find a solution to avoid any future blocking of any possibly trusted emails from outside the Company, which do not consist information security danger.

You further stated that you planned training sessions for the staff that interacts with the clients to remind them the procedures and you have circulated detailed instructions as to how the staff should reply to each type of request, in order to avoid having a similar miscommunication with the clients in the future.

Regarding the access request of Mr. [REDACTED], the following information was gathered –

- On 25 October 2019, Mr. [REDACTED] addressed the initial access request to the official GDPR email on the controller, which was properly received this time.
- On 27 November 2019, a letter was sent to Mr. [REDACTED] answering all his queries and detailed instructions were provided on how to download his data. Mr. [REDACTED] claimed to never have received the letter and on 16 January 2020, the controller created a link through the record management database which contained the data and sent the link to Mr. [REDACTED] by e-mail. On the same day, Mr. [REDACTED] contacted the Customer Support team stating that he was facing a problem with the link. The Customer Support team offered assistance in order to resolve the issue but no feedback was received from Mr. [REDACTED]
- On 24 February 2020 the controller sent a follow up e-mail to Mr. [REDACTED] to check whether he managed to open the link concerning the access request and Mr. [REDACTED] claimed that he never received the link with his data. On 4 March 2020, a new link was created through the database and sent to Mr. [REDACTED]. On 5 March 2020, the controller sent a follow up e-mail to Mr. [REDACTED] to check whether he received the link. No answer was received by Mr. [REDACTED] until today.

Commissioner's assessment

We considered all information available in relation to the case and we have the view that you eventually complied with Mr. [REDACTED] access request. Since you were able to demonstrate credibly that you have fulfilled your obligation to provide information to the complainant by means of the letters of 27 November 2019, 16 January 2020 and 4 March 2020, no further action on your part is necessary.

Furthermore, we take note of the remedial actions taken by the controller to avoid any future blocking of trusted emails and we do not intend to take further action regarding the matter.

We would like to inform you that we keep a record of all the complaints raised with us about the way organisations process personal information. The information we gather from complaints may form the basis for action in the future, where appropriate.

Commissioner
for Personal Data Protection

Deliberation of the Restricted Committee SAN-2020-003 of 28 July 2020 relating to

The Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority), meeting under its Restricted Committee, comprised of [REDACTED]
[REDACTED], members;

Having regard to Convention no. 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and the free movement of such data;

Having regard to amended Act no. 78-17 of 6 January 1978 on information technology, data files, and civil liberties, notably Articles 20 et seq.;

Having regard to Decree no. 2019-536 of 29 May 2019, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and liberties (French Data Protection Act);

Having regard to Deliberation no. 2013-175 of 4 July 2013 on the adoption of Commission Nationale de l'Informatique et des Libertés' internal regulations;

Having regard to Decision no. 2018-076C of 30 March 2018 of the Chair of the Commission Nationale de l'Informatique et des Libertés to entrust the secretary-general with carrying out a verification mission, or having such verification mission carried out by this entity or on behalf of [REDACTED];

Having regard to the Decision of the Chair of the Commission Nationale de l'Informatique et des Libertés appointing a Rapporteur before the Restricted Committee, dated 29 April 2019;

Having regard to the report submitted by [REDACTED] Rapporteur commissioner, notified to [REDACTED] on 23 September 2019;

Having regard to the written submissions from [REDACTED] on 24 October 2019;

Having regard to the Rapporteur's response to these submissions notified on 7 November 2019 to the company's counsel;

Having regard to the new written submissions from [REDACTED]'s counsel received on 22 November 2019 as well as the oral observations made during the Restricted Committee session on 28 November 2019;

Having regard to the other items in the case file;

The following were present during the Restricted Committee session of 28 November 2019:

- [REDACTED] [REDACTED], commissioner, his report having been read;

As representatives of [REDACTED]:
- [REDACTED];

[REDACTED]

The company [REDACTED] having addressed the Committee last;

The Restricted Committee adopted the following decision:

I. Facts and proceedings

1. The company [REDACTED] (hereinafter "the company") is a simplified joint-stock company [REDACTED]
[REDACTED]
2. In 2018, [REDACTED] achieved a net turnover of over EUR 108 million and a negative net income of around EUR 600,000. The same year, the [REDACTED] group, comprised of [REDACTED] SAS and its subsidiaries, achieved a net turnover of around EUR 160 million and a negative net income of around EUR 2 million. The [REDACTED] group employs around 1,000 people.
3. For the requirements of its business, the company operates 16 websites within 13 European Union (EU) countries: France, Spain, Germany, Italy, the Netherlands, Slovakia, Denmark, Poland, Sweden, Finland, Belgium, the Czech Republic and Hungary as well as in the United Kingdom. Two other websites ([REDACTED] and [REDACTED]) are intended for consumers from other countries, paying in euros and dollars.
4. On 31 May 2018, pursuant to the Chair's decision no. 2018-076C, a delegation of the Commission Nationale de l'Informatique et des Libertés (hereinafter "the CNIL" or "the Commission") conducted an investigation within [REDACTED]'s premises. The purpose of this investigation was to check the company's compliance with all of the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "Regulation" or "GDPR") and Act no. 78-17 of 6 January 1978 amended on information technology, data files and civil liberties (hereinafter "Act of 6 January 1978 amended" or "Data Protection Act"). The investigations were especially carried out for the processing of data of prospects and clients and the recording of telephone conversations between customer advisers and customers.
5. During this investigation, the delegation was informed that the company carries out processing aimed at combating fraud and non-payment, during payments made on its websites. When the 3DSecure protocol is not validated, an email is sent to the person having placed the order for them to send proof of residence and a scan of the front of their bank card. Moreover, the company informed the delegation that no retention period had been defined where personal data

is concerned, and that it did not take steps at regular intervals to erase data concerning customers and prospects after a defined period of time

6. The delegation observed that, for the recording of telephone conversations between customer advisers and customers, data subjects calling the company could object to telephone calls being recorded by pressing a key on their telephone.
7. Finally, the delegation found that, when a user creates an account on the company's website, passwords made up of six digits, containing only one type of character, are accepted. The company also explained that account passwords are stored in a production base in hashed form using the MD5 function, with the addition of a salt directly present in the database field related to the corresponding password.
8. Furthermore, following the investigation and by email of 7 June 2018, the company provided the Commission with the additional pieces of evidence requested, particularly a breakdown from the database of the number of customers and prospects who have not signed in, since 2008, to its websites across the different countries in which it operates. The following items were provided by the company:
 - 118,768 customers, whose personal data featured in the database, had not signed in since 25 May 2008;
 - 682,164 customers had not signed in since 25 May 2010;
 - 3,620,401 customers had not signed in since 25 May 2013;
 - 5,790,121 customers had not signed in since 25 May 2015;
 - 25,911,675 prospects had been inactive since 25 May 2015.
9. This breakdown also showed that the company [REDACTED] had over 11 million customer accounts and over 30 million prospects.
10. In addition, by email dated 27 June 2018, the company furnished the CNIL with the new data protection policy for its various websites.
11. Pursuant to Article 56 of the GDPR, the CNIL informed, on 27 July 2018 all of the European supervisory authorities of its competence to act as the lead supervisory authority regarding the cross-border processing carried out by the company and opening the proceedings for the declaration of the authorities concerned on this case
12. In order to investigate these elements, on 18 April 2019, the Chair of the Commission appointed [REDACTED] in the capacity of Rapporteur on the basis of Article 47 of the Act of 6 January 1978, amended, according to its version applicable on the date of his appointment.
13. By email dated 17 May 2019, the company was summoned by the Rapporteur to a hearing pursuant to Article 74 of Decree no. 2005-1309 of 20 October 2005 amended.

14. Following his investigation, on 23 September 2019, the Rapporteur served the company [REDACTED] by court bailiff with a report providing details on the GDPR breaches that he considered had been committed in this case.
15. This report suggested that the Commission's Restricted Committee issue an order to bring processing into compliance with the provisions of Articles 5-1-c), 5-1 e), 13, 32 and 35-1 of the Regulation, and a penalty after a period of three months following notification of the Restricted Committee's deliberation, as well as an administrative fine. It also suggested that this decision be rendered public and that the company no longer be identifiable by name upon expiry of a period of two years from its publication.
16. A summons to the Restricted Committee session of 28 November 2019 was also appended to the report informing the company that it had a period of one month to provide its written submissions.
17. On 23 October 2019, the company produced submissions through the intermediary of its counsel. The Rapporteur responded to these submissions on the following 7 November.
18. On 22 November 2019, the company produced new submissions in response to those of the Rapporteur.
19. During the Restricted Committee session of 28 November 2019, the company and the Rapporteur presented their oral observations.
20. The draft decision adopted by the Restricted Committee was communicated to the European supervisory authorities concerned on 16 February 2020 in accordance with Article 60.4 of the GDPR. In its draft decision, the Restricted Committee ruled on the breaches proposed by the Rapporteur in its report and discussed by the parties in respect of the adversarial principle, i.e. breaches of articles 5-1-c), 5-1-e), 13, 32 and 35-1 of the GDPR; no breach of Article 6 of the GDPR and of the Directive 2002/58/EC of the Parliament and of the Council, known as the "ePrivacy Directive", having been raised by the Rapporteur.
21. On following 13 and 17 March, the supervisory authorities of Italy, Portugal and Lower Saxony expressed relevant and reasoned objections on the draft decision. The Restricted Committee decided to revise its draft decision to take into account these objections. As these objections did not propose to depart from the draft decision by taking into account a new factual circumstance, to add a breach or to aggravate the nature of the corrective measure initially proposed, the Restricted Committee decided not to communicate them to the rapporteur and to [REDACTED].
22. The revised draft decision was submitted to the supervisory authorities concerned on 25 June 2020.

II. Reasons for the decision

A. On the breach of the principle of data minimisation (requirement to ensure that data is adequate, relevant and limited to what is necessary)

1. The recording of telephone calls

23. Article 5-1. (c) of the Regulation provides that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*".
24. **Firstly**, the Rapporteur submits that the full and permanent recording of telephone calls from customer service employees appears excessive with regard to the purpose of assessment of employees by the company.
25. The company argues that telephone recordings are neither permanent nor systematic given that customers can object to the call being recorded. It also considers that full recording of telephone conversations is proportionate to the purposes of assessing and training employees pursued by the company. Lastly, it maintains that the Rapporteur is incorrect in asserting that recording telephone calls is an excessive measure as the person responsible for training usually only listens to one recording a week per employee, whereas, according to the Company, this average is likely to evolve in line with its needs. It states that the number of recordings that the trainer should be able to listen to should be higher than the number of recordings that he actually listens to.
26. First, the Restricted Committee notes that although some customers object to their telephone call being recorded, the company carries out processing to record all of its employees' telephone calls, without said employees being able to object. It further considers that the company does not justify its need to record the whole of telephone conversations with the customer service department, with regard to the processing purpose, i.e. training employees. The Restricted Committee notes that, during its hearing dated 19 June 2019, the company indicated that the person in charge of such training only usually listens to one recording per week per employee. Furthermore, while the company asserted during the session of 28 November 2019 that the rate of recording of telephone conversations had been reduced from 100% to 30%, it does not provide any proof of this.
27. Although the number of recordings can vary depending on each employee and on circumstances, particularly as regards employees' training needs, the Restricted Committee considers that the company does not prove that it has limited, both in the past and for the future, the recording of employees' telephone conversations to what is necessary in light of the purpose pursued. Yet, a data controller cannot process personal data without checking that such processing is necessary in light of its needs, *a fortiori* when it is based on a particularly intrusive measure for employees.

28. In light of this, the Restricted Committee therefore considers that a breach to Article 5-1-c) of the GDPR has been committed.
29. **Secondly**, the Rapporteur criticises the company for not having taken measures to avoid the recording of customers' bank details during telephone calls with the company. He also considers that the measure suggested by the company following the hearing, which consists of erasing calls relating to orders placed by phone with payment by bank card on a daily basis, is not satisfactory given that the processing of bank data for a whole day is not justified in light of the purpose of the processing, which is staff assessment. He reminds the company that the purpose of processing of bank details is to complete a payment and that such data should not be recorded by the company, even for only a day, once payment has been confirmed.
30. The company argues that the daily erasure of bank data recorded during telephone conversations decided following the hearing of 19 June 2019 ensures that data are stored in accordance with the principle of minimisation. It specifies that the implementation of a measure to suspend recording when a customer's bank details are provided would require developing complex technical tools and would incur significant financial and human costs.
31. The Restricted Committee notes that, at least up until 19 June 2019, the company recorded the bank details of customers placing orders by telephone when recording its employees' conversations for training purposes and stored such data in clear text in its database for fifteen days.
32. It notes that bank details are data which, due to their nature and the associated risks of fraud, must be granted greater protection by data controllers. As highlighted by the Rapporteur, use of such data by unauthorised third parties for fraudulent payments is likely to prejudice data subjects.
33. The Restricted Committee observes that the company recorded and stored data for which it had no use in light of the purpose pursued by the processing in question, i.e. the training of employees.
34. In light of this, it therefore considers that a breach to Article 5-1-c) of the GDPR has been committed.

2. Data collected to combat fraud

35. **Firstly**, the Rapporteur argues that the company disregards the principle of data minimisation by storing supporting documents provided by customers such as copies of national identity cards, for anti-fraud purposes, when they are not required.
36. The company states that storage of a document provided spontaneously by an individual is not excessive. It considers that it can store copies of national identity cards provided by individuals spontaneously given that the CNIL indicates in its practical guide on "online purchases" that a data

controller may ask for documentary proof of identity and/or address in order to make sure of the cardholder's identity.

37. The Restricted Committee notes that, during the hearing of 19 June 2019, the company informed the CNIL that it was asking customers located in France to provide a copy of proof of address and a scan of their bank card for anti-fraud purposes. However, it informed the Commission that although it does not request a copy of an identity card, some individuals provide such a document and that in this case, it stores this document for six months, the same period as for the other documentary proof provided to it.
38. The Restricted Committee notes that a copy of an identity card may constitute appropriate documentary proof for the purposes of combatting fraud. Consequently, given the purpose of the processing carried out by the company and the residual nature of the number of copies of identity cards processed by the company, it considers that, in this case, there is no reason to observe a breach.
39. **Secondly**, in his report, the Rapporteur highlighted that, for anti-fraud purposes, the company collected copies of "health cards" ("tessera sanitaria") and valid identity cards in Italy. He accused the company of not being able to specify during the hearing why the collection of such a document was necessary for anti-fraud purposes. The Rapporteur subsequently noted that information provided by the company by which it declared that its statements made during the hearing of 19 June 2019 were false and that it actually only asked customers to provide their identity card to the exclusion of all other documentary proof. The company also stated that following a communication error, from 27 June to 18 July 2019, the company's marketing department requested that customers provide a copy of said health card, but that this practice had been brought to an end and that the documents thus collected have been erased. The Rapporteur therefore considered that there was no longer a need to take this fact into account as regards the abovementioned breach.
40. The Restricted Committee notes that the Italian "health insurance card" contains a range of information concerning its holder, namely his or her first and last names, gender, tax code and place of birth which, for citizens born in Italy, corresponds to the municipality of birth and, for foreign nationals, to the country of birth. It can also be deduced from the card's expiry date that the holder has a permit to stay in Italy.
41. It considers that the communication of two documents allowing to prove the identity of the person in the context of combating fraud, namely the "health insurance card" and the identity document, was excessive and irrelevant under article 5-1-c) of the GDPR. Indeed, it appears that only the collection of the identity card was relevant to the purpose of the processing operation. In the present case, the collection of the "health insurance card" containing more information than the identity card, not relevant in the context of combating fraud, was excessive. In this regard, the Restricted Committee notes that the company acknowledges that such collection was not necessary, as it stopped in July 2019. The Restricted Committee considers that even if the company would have collected such a document only for a limited period of three weeks, such elements

constitute a breach of the obligation of the data controller to process only data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in accordance with the data minimisation principle.

42. The Restricted Committee considers that a breach of Article 5-1-c) of the GDPR has been committed as regards these events.

B. On the breach of the requirement of data storage limitation

43. Article 5-1-e) of the Regulation provides that personal data shall be: "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*".
44. **First**, the Rapporteur observed that, during the investigation of 31 May 2018, the company informed the CNIL that no storage period had been defined for customer and prospects' data and that it did not regularly erase or archive such data after a set period. During the hearing of 19 June 2019, the company informed the Rapporteur that it had set out a five year storage period for such data in an active database as from the date on which customers and prospects were last active, which could, for example, be connection to their customer account, a click on a newsletter or the opening of a newsletter.
45. To determine the number of customers and prospects to be taken into account, those located in the United Kingdom should also be included given that this State was a member of the European Union at the time of the events in question and that the GDPR therefore applies. In addition, as part of the withdrawal agreement between the European Union and the United Kingdom, a transition period has been agreed during which European Union law will continue to apply in the United Kingdom.
46. The readings taken by the company at the investigation delegation's request, showed that the company stored the data of 118,768 customers who had not connected to their account since 25 May 2008, that of 682,164 customers who had not connected to their account since 25 May 2010 and the data of 3,620,401 customers who had not connected to their account since 25 May 2013.
47. The Restricted Committee deduced that, at least up until the database count of 7 June 2018, the company stored a significant amount of data relating to customers who had not connected to their account in over ten years.
48. Furthermore, the fact that the company alleges that only the legal director had access to customer's stored data is of no significance as the storage period has no relation to access.

49. As regards prospects, the Rapporteur considers that the company does not prove the need to apply a five-year data storage period as from the date of last contact made by the latter.
50. However, the company argues that the five-year storage period for such data is appropriate given the specificity of its general e-commerce platform. Furthermore, it is known that certain prospects connect to the website to look at what is on offer after four years of inactivity.
51. The Restricted Committee notes that, in June 2018, in the different European Union countries in which the company performed its business and in the United Kingdom, the company stored the data of over 25 million prospects having been inactive since 25 May 2015, i.e. for over three years. Furthermore, as a striking example, the data of 4,801,596 prospects in Spain having been inactive for over three years, that of 5,616,503 prospects in Italy and that of over 12 million prospects in France were stored. The Restricted Committee notes that after having informed the CNIL's departments that their data were stored without period limitation, the company indicated during the hearing that it now stored such data for five years as from the date of last contact, even though it states that it no longer contacts them after two years of inactivity. The Restricted Committee considers that the company has not demonstrated how the storage of prospects' data, as individuals having never placed an order on the company's website or as former customers whose data are used for prospection purposes after their commercial relationship has ended, is necessary after the period of two years during which it carries out its marketing campaigns. Under such conditions, the company stores prospects' data for a period exceeding that which is necessary in light of the purposes for which they are processed. Indeed, the company stated that it sends emails to carry out its commercial prospection to the prospects only during two years.
52. On this point, the Restricted Committee considers that in this case, the data retention period of two years is proportionate for the purpose for which the personal data are processed. This retention period answers to the company's aspiration to promote, as any merchant, its products to its former customers and to people who have not objected to receiving such messages. The company also specifies that people can unsubscribe, at any time, to the reception of prospecting messages. However, the retention period set up by the company for prospects data, i.e. five years, exceeds what is necessary for the purposes for which they are processed.
53. The Restricted Committee therefore considers that the company has violated the provisions of Article 5-1 e) of the GDPR.
54. **Secondly**, the Rapporteur criticises the company for setting the opening of a marketing email as a starting point for the storage period for prospects' data.
55. The Restricted Committee notes that prospects' data enables data controllers to send messages, by email for example, to individuals showing an interest in its products or services. The Commission considers in this respect that when the starting point of the data storage period is the date of last contact made by the prospect, this must be an event demonstrating the individuals' interest in the message received, such as a click on the hypertext contained in an email. However, the mere

opening of an email cannot be considered as contact made by the prospect, given that such an email may be opened involuntarily due to the way in which the email software used works or by mistake.

56. The Restricted Committee therefore considers that the company cannot consider that the mere opening of a marketing email by an individual may trigger the start of the storage period for prospects' data and therefore store such data without breaching the principle of data storage limitation when prospects have not shown interest in the company's products or services by taking clear action for several years.
57. **Thirdly**, the Rapporteur maintains that, on expiry of the storage period for customers' data, the company does not erase all data stored, but keeps customers' email address and passwords under a pseudonymised format, which does not ensure compliance with the principle of data storage limitation.
58. The Company maintains that "*anonymisation*" of former customers' email addresses is carried out via a procedure based on a SHA256 technology and that decryption of data that has been hashed thereby requires highly sophisticated technical skills. It therefore considers that inactive customers' data is "*undecryptable and therefore anonymous*".
59. The Committee notes that after a customers' period of inactivity, the company erases certain data, i.e. the customers surname, name and date of birth, but stores other data such as his/her email address and password which are hashed by an algorithm and transferred to another table. By doing so, the company wishes to enable a customer to reconnect to his/her account using the same login and password as those used when creating the account, after the data storage period set out.
60. The Restricted Committee considers that the data belonging to its former customers, although hashed, are not anonymised but pseudonymised and individuals could therefore be identified.
61. The company submits that the email addresses and passwords of its former customers are hashed using a particularly strong SHA256 algorithm which anonymises data.
62. The Restricted Committee notes that the SHA256 algorithm is a hash function ensuring the integrity of the personal data processed by the company. Although it is, to date, a function which cannot be reversed and is therefore considered to ensure a sufficient level of data security by the National Cybersecurity Agency of France (ANSSI) and by the CNIL, it does not anonymise data and therefore justify their indefinite storage by a data controller.
63. Consequently, the Restricted Committee considers that the company stores the data in question for a period exceeding that which is necessary in light of the purposes for which they are processed. In this respect, it notes that the company itself states that the purpose of taking such a measure is to enable its customers to reconnect to their account, even though the data is meant to have been erased. Former customers' personal data must be definitely erased on expiry of the storage period

of such data in an active database or in an archive data based, once legal requirements have expired, and cannot be stored for a hypothetical future use.

64. The Restricted Committee therefore considers that the company has, once again, breached the provisions of Article 5-1 e) of the GDPR.

B. On the breach of the requirement to inform data subjects

65. Article 13 of the GDPR requires that the data controller, at the time when data are obtained, provide information relating to its identity and contact details, the contact details of the data protection officer, the purposes of the processing and its legal basis, the recipients of the personal data, where applicable the transfer of personal data, the period of storage of the personal data, the rights of data subjects and the right to lodge a complaint with a supervisory authority.
66. **As regards customers**, the Rapporteur accused the company of not informing customers, in the data privacy policy accessible on the company's website and via a link on the form to create an account, that their data are transferred to Madagascar in the context of telephone calls. He also criticised the company for only citing one legal basis in these documents for all of its processing, i.e. consent, when several processing operations were based on a different legal basis.
67. In his submissions of 7 November 2019, the Rapporteur noted that despite the company's assertions, its privacy policy had not been corrected to include the transfer of data to Madagascar.
68. As regards the legal bases of processing, the company affirmed that it based its processing on data subjects' consent, which, in its opinion, it could not be reproached for given that this legal basis provides data subjects with greater protection and that, as a result, a breach to the lack of information of data subjects could not be held against it for these events.
69. The Restricted Committee notes that it results from the company's statements on the various processing operations carried out that several of them, i.e. for example the fight against fraud or the processing carried out for purchases placed on the company's website, could not be based on data subjects' consent but rather, as indicated by the Rapporteur, on a contract or on the legitimate interests pursued by the company. Recalling that recital 41 of the GDPR requires that the legal basis of processing be "*clear and precise*", it considers that the company cannot only refer in its data privacy policy to the legal basis of consent for all processing carried out.
70. Consequently, although the company has indeed included information on the legal basis, as required by texts, and taken the care to select the basis that provides in its view the most protection to data subjects' rights, the Restricted Committee reminds it that Article 13 of the GDPR requires granular information relating to the legal basis of each processing operation. It can therefore only note that the company has not fully complied with the provisions of this article by abstaining to provide, for each processing operation carried out, the corresponding legal basis in its privacy policy.

71. Furthermore, the Restricted Committee notes the changes made on its website as regards the transfer of data to Madagascar. However, it considers that a breach to Article 13 of the GDPR was committed up until 18 November 2019, the date on which the company stated that it had made changes to its website.
72. **As regards employees**, the Rapporteur criticises the company for not having informed them individually of the recording of their telephone calls.
73. The company submits that employees are informed of the recording of telephone calls with customers, via several documents, such as a certificate of presence "information project telephone recording" dated 14 January 2016, a document dated May 2014 and performance assessment forms dated 2017. The company also provided statements from three customer advisors confirming that they had read the document dated 14 January 2016, that they have understood the purpose of such recording and that they may contact the legal department for further information.
74. The Restricted Committee recalls that informing employees of the use of measures to listen to and record telephone conversations in the work place is vital and is related to the fair and transparent nature of any processing implemented by a data controller. As indicated in recital 39 of the GDPR, *"The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used"*.
75. The obligation of transparency requires the company to provide information on such a measure to each employee, with the former unable to only provide information once, as in this case in 2016, which is not provided to new employees hired subsequently.
76. Moreover, the Restricted Committee also noted that Article L. 1222-4 of the French Labour Code provides that *"no information personally concerning an employee may be collected by a measure which has not previously been brought to his or her attention"*. Furthermore, the Commission has repeated on several occasions, including in a guide for employers and employees available on its website and in recommendation no. 2014-474 of 27 November 2014 relating to the recording of phone calls at the work place, that employees must be provided a certain amount of information relating to the processing carried out by employers.
77. Lastly, the Restricted Committee notes that the documents produced by the company do not allow it to provide employees with information on the purposes pursued by the processing, on the legal basis of the measure, on the recipients of the data produced by the measure, on the data storage period, on their rights, particularly to access the data concerning them and on the possibility of lodging a claim with the CNIL, ensuring the full information of employees pursuant to Article 13 of the GDPR.
78. In light of the above, the Restricted Committee therefore considers that a breach to Article 13 of the GDPR has been committed.

C. A breach of the requirement to ensure data security

1. The absence of security regarding passwords providing access to customer accounts

79. Article 32-1 of the Regulation provides that: "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*" including "*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*".
80. Thus, pursuant to Article 32-2 of the GDPR, the data controller must take account of the risks that are presented by processing, in particular from destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, whether accidentally or unlawfully.
81. During the investigation of 31 May 2018, the CNIL delegation observed that the individuals wishing to create a user account on the company's website could create a password comprised of six characters containing only one character category. During the hearing of 19 June 2019, the company specified that since the CNIL investigation, a measure to block the account for one minute had been put in place, after 19 unsuccessful attempts to access an account from a single IP address in less than one minute.
82. In its defence, the company submits that it has changed the rules for the creation of passwords for accounts and now requires that its customers create passwords comprised of at least eight characters. It also questions the CNIL's recommendations on the topic and maintains that the technical recommendations in terms of password security in deliberation no. 2017-190 of 22 June 2017 of the Commission have been disputed by cybersecurity experts. Claiming that overly complex rules have resulted in the standardisation of passwords, it preferred to opt for requiring shorter and simpler passwords, with these being less predictable for potential attackers, with the risk being based on human logic.
83. The Rapporteur maintains that passwords comprised of six or eight characters, without any complexity criteria, are not strong enough and do not ensure the security of the data processed by the company. He considers that such passwords to not prevent attacks "by brute force" which consist of successively and systematically testing many passwords and can therefore compromise associated accounts and the personal data they contain.
84. The Restricted Committee considers that, contrary to what the company states, the length and complexity of a password are elementary criteria to assess the strength of the latter. It reminds the company that in order to ensure a sufficient level of security and meet password strength requirements, when authentication is based only on an identifier and a password, the password must contain at least twelve characters – containing at least one uppercase letter, one lowercase

letter, one number and one special character – or the password must contain at least eight characters – containing three of these four character categories – and be completed by an additional measure such as the timing out of access to an account after several failed attempts (temporary suspension of access for an increasing period of time for each attempt), the implementation of a mechanism to prevent automated and intensive attempts (e.g.: "captcha") and/or the blocking of the account after several unsuccessful authentication attempts.

85. The Restricted Committee notes that the need for a strong password is also underlined by ANSSI, which states that "*a good password is above all a strong password, i.e. difficult to find even using automated tools. A password's strength depends on its length and the number of possibilities that exist for each character comprising it. A password comprised of lowercase letters, uppercase letters, special characters and numbers is technically more difficult to find than a password comprised of only lowercase letters*".
86. In this case, it considers that the strength of a password comprised of eight characters and only one category of characters is very weak and that the company does not, at any time, demonstrate how a short and simple password would be likely to better resist an attack by brute force than a password comprised of more characters and several categories of characters.
87. As a consequence, the Restricted Committee considers that the passwords put in place by the company to access customer accounts created on its website do not meet requirements in terms of strength.

2. Request to provide a copy of the payment card

88. During the investigation of 31 May 2018, the delegation observed that the company requested that its customers provide it with a scan of the bank card used on ordering, for anti-fraud purposes. For its customers in France, an email specifying "*out of the 16 numbers on the front, please make sure that at least the first 4 and last 4 are clearly visible, and that the expiry date and cardholder's name are also legible*" was therefore sent to data subjects. Emails making this request were also sent to individuals placing orders on the Italian, Spanish, Hungarian, Slovakian, Danish and Greek websites. It was noted that the company stored the scans of un-blanked bank cards.
89. In this regard, the Rapporteur therefore considers that the company's email sent to individuals, particularly to French citizens, prompts customers to submit a full copy of the payment card instead of encouraging them to hide a minimum of numbers on it.
90. It was also observed that payment card scans are stored by the company in clear-text for six months from recording of the documents, in case of dispute.
91. By letter of 28 June 2019, the company stated that an online platform dedicated to sending supporting documents would be set up at the end of August 2019. Furthermore, the company maintains that it was authorised by the CNIL to carry out processing the purpose of which is to combat fraud and that it may validly collect bank card expiry dates and truncated numbers.

92. **First**, the Restricted Committee notes that the company was indeed authorised by a CNIL deliberation of 2 July 2009 to process truncated bank card numbers as well as the expiry date, for processing the purpose of which is to combat fraud. However, it has been demonstrated that the company processed the copies of customers' bank cards containing all numbers, when it was only authorised to process a truncated part of these. The Restricted Committee therefore considers that the authorisation issued by the CNIL cannot justify the processing of all of customers' bank card numbers.
93. **Secondly**, the Restricted Committee notes that the CNIL delegation observed that the measures put in place by the company enabled customers to send photographs or scans of their bank cards containing all bank card numbers in clear text by unencrypted email from their mailbox, or that such data were stored, as was the documentary proof requested for the purposes of combatting fraud, for six months in clear text in the database.
94. Under such conditions, the Restricted Committee considers that, at least up until August 2019, the company did not take security measures to ensure the security of its customers' bank data.
95. Based on these elements, the Restricted Committee considers that Article 32 of the Regulation has been breached.

D. On corrective measures and their publicity

96. Pursuant to paragraph III of Article 20 of the Act of 6 January 1978 amended:

"Where the data controller or their data processor does not comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this Act, the Chair of the Commission Nationale de l'Informatique et des Libertés may also, where necessary and after having sent the warning provided for in Paragraph I of this Article or, where necessary in addition to the notice provided for in Paragraph II, refer to the Commission's Restricted Committee to pronounce, following an adversarial procedure, one or several of the following measures: [...] "

2) An order to bring processing into compliance with the obligations arising from this Act or from the aforementioned Regulation (EU) 2016/679 of 27 April 2016 or to respond to the requests presented by the data subject with a view to exercising his or her rights, which may be completed by a periodic penalty payment not exceeding €100,000 per day overdue as from the date set by the Restricted Committee, save for cases in which the processing is carried out by the State; [...]

7) Save for cases in which the processing is carried out by the State, an administrative fine that cannot exceed EUR 10 million or, where it is carried out by a company, 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In the cases mentioned in paragraphs 5 and 6 of Article 83 of aforementioned Regulation (EU) 2016/679 of 27 April 2016, these ceilings shall be increased respectively to EUR 20 million and 4% of said

turnover. The Restricted Committee shall take into account, when determining the amount of the fine, the criteria specified in said Article 83."

97. Article 83 of the GDPR provides that:

"1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58 (2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the type, seriousness and duration of the breach in light of the type, scope or purpose of the processing in question, as well as the number of data subjects affected or the level of damage they have suffered;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58 (2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."

98. **Firstly**, as regards the fine proposed by the Rapporteur, the company submits that it has never been sentenced by the CNIL, that it had few frameworks prior to entry into force of the GDPR and that the Commission had announced a tolerance period as concerns new breaches to the GDPR, such as data minimisation or pseudonymisation.

99. The Restricted Committee considers that in the present case, the abovementioned infringements warrant that an administrative fine be issued against the company for the following reasons.

100. First, it notes that, contrary to the company's assertions, the breaches in question mostly concern requirements that Act no. 78-17 of 6 January 1978 amended already imposed on data controllers and which do not arise from the GDPR, including as regards the principle of data minimisation and storage limitation. Furthermore, it reminds the company that the questions relating to data pseudonymisation had already been asked well before entry into force of the GDPR.
101. It further notes that several of these breaches concern employees and their right to receive information on the processing of their personal data. Here again, the Restricted Committee reminds the company that this is not a new requirement introduced following entry into force of the GDPR.
102. Lastly, it underlines that bank data are data which must be the subject of particular care from data controllers and that the Commission has continued to assist them on this topic for many years.
103. **Secondly**, the company highlights its cooperation with the Rapporteur and the measures put in place, as well as some sanctions previously issued by the Restricted Committee. It also considers that it cannot be reproached a lack of speed when the hearing took place one year after the investigation carried out within its premises and when no formal notice was issued to it within this period.
104. The Restricted Committee notes that although several measures were put in place by the company in order to correct certain breaches in whole or in part, these were only adopted following the CNIL's investigation of 31 May 2018 as regards the implementation of storage periods for customers' and prospects' data, and only following the hearing of 19 June 2019 and the report for the erasure of recording containing customers' bank details and the information of data subjects on the website as regards the transfer of their data outside of the European Union.
105. The Restricted Committee further considers that the seriousness of some breaches is characterised. More specifically as regards the breach relating to the recording of telephone conversations, the Restricted Committee notes that the company recorded full telephone conversations had by its employees for several years, when it had no reason to do so and that such processing can be likened to constant surveillance. It also notes that the information provided to employees on the implementation of measures to record phone calls was particularly lacking, being either incomplete prior to 2016, or non-existent for employees hired by the company after this date.
106. Furthermore, the seriousness of the breaches is characterised given the specific category of personal data processed by the company, i.e. bank data which are considered as data exposing data subjects to a risk of fraud, and thereby of prejudice, and must as such be the subject of particular vigilance. Lastly, the Restricted Committee also considers that the seriousness of the

breaches is characterised due to the number of data subjects concerned by the breaches, particularly as regards data storage periods which affected several thousands of data subjects.

107. The company goes on to argue that it is a medium-sized company and that it operates in a particularly competitive sector. It considers that a high administrative fine would affect its financial health and its market position.
108. In this respect, the Restricted Committee considers that the company is an established e-commerce player and that, being founded well before the entry into force of the GDPR, it could not ignore the basic rules of data protection.
109. In addition, the Restricted Committee recalls that Article 83, paragraph 3 of the Regulation provides that in the case of several infringements, as is the case here as four breaches have been established, the total amount of the fine cannot exceed the amount specified for the gravest infringement. Given that the company is accused of infringing Articles 5 and 12 of the Regulation, the maximum amount of the fine that could be imposed is 20 million euros or 4% of the annual worldwide turnover, whichever is higher.
110. However, when determining the amount of the fine issued, the Restricted Committee also takes into account the measures that the company has taken during the sanction proceedings to ensure partial compliance and its cooperation with the Commission's departments.
111. **Thirdly**, as regards the need to issue an injunction, the company considers that formal notice without periodic penalty payments would be more suited given the speed already observed in ensuring compliance for several breaches.
112. While it does not ignore the steps taken by the company to ensure compliance with the GDPR, the Restricted Committee considers that the company did not prove, on the day on which the investigation was closed, the full compliance of the processing carried out under Articles 5-1-c), 5-1 e) 13 and 32 of the Regulation.
113. The company having failed to ensure compliance as regards these breaches, there is reason to issue an injunction.
114. **Fourthly**, the Restricted Committee considers that the publicity of the sanction is justified in light of the importance of the issues raised as regards employees, as well as the nature of the data in question, when the company is an important player in the sector in which it operates.
115. As a result of the above and the consideration of the criteria set out in Article 83 of the GDPR, an administrative fine of 250,000 euros, an injunction with periodic penalty payments and an additional sanction of publication for a period of two years are justified and proportionate.

FOR THESE REASONS

The Restricted Committee of the CNIL, after having deliberated, decides:

- to impose on [REDACTED] an injunction to bring processing in compliance with the requirements arising from Articles 5-1 c), Article 5-1 e), 13 and 32 of Regulation no. 2016/679 of 27 April 2016 on data protection, and in particular:
 - with respect to the breach of the principle of personal data minimisation:
 - prove the end of the non-punctual and non-random recording of advisors' telephone conversations when the purpose pursued is their training or assessment;
 - with respect to the breach of the principle of data storage limitation, define and implement a policy concerning the period for which the data concerning customers and prospects will be stored, which shall not exceed what is necessary for the purposes for which they are collected and processed, and particularly:
 - justify the procedure set up for the intermediate archiving of customers' personal data, after sorting the relevant data to be archived and deleting irrelevant data, as well as the starting point for such archiving;
 - justify the restriction of employees' access to personal data contained in the active database to only persons needing to have such data;
 - no longer process prospect data beyond the period of time at the end of which the company stops contacting them (two years in the present case) and no longer take the simple opening of an email as the last point of contact made by prospects;
 - no longer retain the email addresses and hashed passwords of former customers at the end of a set period of inactivity and carry out a purge of such data retained by the company up to the date of the Restricted Committee's deliberation;
 - justify that data concerning customers is deleted after the set period of inactivity, which the company shall have to justify, and that data concerning prospects is deleted after two years of inactivity;
 - with respect to the breach of the requirement to inform data subjects:
 - inform employees about the setup of a system for recording telephone conversations, particularly bearing on the intended purposes, the legal basis of the system, the recipients of the data from the system, the data retention period, the rights of employees, particularly to access personal data, and the possibility of lodging a complaint with the CNIL;
 - provide customers with full information, by providing information on the different legal bases of the processing implemented by the company;
 - with regard to the breach to the obligation to ensure personal data security, take any measure, for all personal data processing carried out, to ensure the security of such data and to prevent unauthorised third parties from accessing it pursuant to Article 32 of the GDPR, in particular:
 - implement a restrictive password management policy, as regards customer accounts, according to one of the following arrangements:

- passwords shall be composed of at least twelve characters, containing at least one uppercase letter, one lowercase letter, one number and one special character;
 - passwords shall be composed of at least eight characters, containing at least three of the four character categories (uppercase letters, lowercase letters, numbers and special characters) and shall be completed by a complementary measure such as the timing out of access to an account after several failed attempts (temporary suspension of access for an increasing period of time for each attempt), the implementation of a mechanism to prevent automated and intensive attempts (e.g.: "captcha") and/or the blocking of the account after several unsuccessful authentication attempts (maximum of ten);
- associate the injunction with a periodic penalty payment of 250 (two hundred and fifty) euros per day of delay on expiry of a period of 3 (three) months following notification of this deliberation, with the documentary proof of compliance being sent to the Restricted Committee within this period;
 - for the breaches to Articles 5-1 c), 5-1 e), 13 and 32 of the GDPR, impose on [REDACTED] [REDACTED] an administrative fine of 250,000 (two hundred and fifty thousand) euros;
 - to make its decision public on the CNIL website and on the Légifrance website, which will no longer identify the company by name upon expiry of a period of two years from its publication.

The Chair

[REDACTED]

This decision may be appealed to the French Conseil d'État within two months of its notification.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2023-03-23, no. IMY-2022-9186. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-9186

Date of decision:
2023-03-23

Decision pursuant to Article 60 under the General Data Protection Regulation – MAG Interactive AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that MAG Interactive AB has processed personal data in breach of Article 12(3) of the General Data Protection Regulation (GDPR)¹ by not having accommodated the complainant's request for erasure made on 4 August 2021 without undue delay, and first on 26 November 2021.

The Swedish Authority for Privacy Protection issues a reprimand to MAG Interactive AB pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 12(3) of the GDPR.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding MAG Interactive AB (the company) due to a complaint, mainly to investigate whether MAG Interactive AB has received and handled the complainant's request for erasure in accordance with Articles 12 and 17 of the GDPR. The complaint has been submitted to IMY, as lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, France, Ireland, Norway, Poland, Germany and Austria.

The complaint

The complainant has mainly stated the following. The complainant requested erasure of its account in the 'Quiz Duell' app in July 2021. Since no deletion had been carried out, the complainant posted a Google Play rating to bring it to the attention of the

Postal address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail:
imy@imy.se
Phone:
08-657 61 00

¹ Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

company. On 30 August 2021, the complainant received a reply to the made post, in which the complainant was referred to contact the company at newqdsupport@maginteractive.com. The complainant sent a message to that email address on 8 September 2021 and reminded of the made request. On 7 and 16 October 2021, the complainant reminded again of the request. In response to the email of 16 October 2021, the complainant received a standard reply from the company. On 16 October 2021, the complainant's request had still not been accommodated.

What the company has stated

In its statement from 7 November 2022, the company essentially stated the following. The Company is the data controller for the processing to which the complaint relates.

The Company's description of the events surrounding the complainant's request for erasure

On 4 August 2021, the complainant requested to have his data deleted from the game Quiz Duell. The request was made directly in the game and was received by the company. The request should have been processed automatically on 18 August 2021 but did not for the reasons set out below.

On 30 August 2021, the complainant submitted a review on Google Play and complained, inter alia, that deletion had not taken place. The company has a built-in function in the games to communicate with support, but the complainant had either not seen it or chose not to use that feature. On 31 August 2021, the company's support replied and asked the complainant to send an email to a specified support address for getting help to find out what went wrong.

The complainant then claims that an email was sent to the that email address on two occasions (8 September and 7 October 2021) but the company has no listing in its support system, ZenDesk, that they have received any emails from the complainant. The complainant also claims that it did not receive a response from the company's support, which also indicates that the company has never received any emails from the complainant. The support will respond to all incoming issues. What has gone wrong here, if the complainant has written the wrong email address or if the complainant's email stuck in any spam filter, the company does not know but everything indicates that the complainant's email unfortunately did not arrive.

On 16 October 2021, the complainant emailed one of the company's email addresses with an autoreply that has instructions on how to request deletion of data and how to contact support. That email has been received by the company and the company has also responded to it automatically on the same day.

On 22 November 2021, the company discovered a system problem that led to the failure to erase the data of some persons as they were supposed to be. The error was fixed. On 26 November 2021, the complainant's data was deleted by the company.

What the company states as a reason why the applicant's request for erasure was not handled automatically

During the summer of 2021, the company had a system problem that led to users being stuck in a queue and not deleted as they would. The complainant was one of those users, which resulted in the complainant's data not being deleted on 18 August

2021 as intended. The problem was detected on 22 November 2021 and the error was promptly addressed. The users stuck in the queue were then processed automatically. Finally, on 26 November 2021, the complainant's data was deleted. The error was not detected until both the erasure deadline and the deadline for delay had expired. The user should have been informed of the deletion once it occurred and has also been informed retrospectively, on 30 October 2022.

The company will provide information to all affected persons they can still reach, including the complainant, with an explanation of what happened, regret the delay and provide a further confirmation that their data has been deleted.

The company also states that in connection with the discovery of the problem, they also expanded their monitoring system to cover also this error case, which means that the company's operating staff receive a text message regardless of the time of day if a similar problem occurs. There has not occurred any similar case since then.

Statement of reasons for the decision

Applicable provisions, etc.

Pursuant to Article 17(1) of the GDPR, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the conditions listed in this Article exists, for example if the data are no longer necessary for the purposes for which they were collected or if the consent for processing is withdrawn.

Pursuant to Article 12(3) of the GDPR, upon request, the controller shall provide the data subject, without delay and in any event no later than within one month of receipt of the request, with information on the measures taken pursuant to, inter alia, Article 17. That period may be extended by two months further, if necessary, taking into account the complexity of the request and number of requests received. The controller shall inform the data subject of such an extension within one month of receipt of the request and shall state the reasons for the delay.

Assessment of IMY

MAG Interactive AB has stated that the request made by the complainant on 4 August 2021 was received on the same day and completed on 26 November 2021, i.e. approximately 3 months and 3 weeks after it was made. It did not state that it had to extend the time-limit for handling the complainant's request, nor did the company notify the complainant of such an extension.

MAG Interactive AB has thus acted in breach of Article 12(3) of the GDPR by failing to comply with the complainant's request for deletion made on 4 August 2021 without undue delay as it was processed first on 26 November 2021. What MAG Interactive AB have brought forward, that the reason for the delay concerns a system problem, does not lead to any different assessment.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. Depending on the

circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be taken into account when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The infringement in question, which the supervision covers, has affected one person and has occurred due to a temporary system problem at MAG Interactive AB. The company states that it has taken measures to prevent similar problems from occurring. Against this background, IMY considers that this are minor infringements within the meaning of recital 148 which results in MAG Interactive AB being given a reprimand under Article 58(2)(b) of the GDPR for the infringement found.

This decision has been taken by the specially appointed decision-maker, legal advisor [REDACTED], following a presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) draft decision 2023-03-31, no. DI-2020-10549. Only the Swedish version of the decision is deemed authentic.

Ref no:
2020-10549,
IMI case no. 134686

Date of decision:
2023-03-31

Date of translation:
2023-03-31

Decision under the General Data Protection Regulation – CDON AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that CDON AB has processed personal data in breach of:

- Article 5(1)(c) and Article 12(6) of the General Data Protection Regulation (GDPR)¹ by requesting more information than necessary from the complainants in complaint 1-3 and 6-7 when they requested to have their personal data deleted without the processing being necessary to confirm their identity.
- Article 12(2) of the GDPR by using a burdensome verification method against complainants in complaint 1-3 and 6-7 without any further justification. Consequently, CDON AB did not sufficiently facilitate the complainant's exercise of their right to erasure under Article 17 of the GDPR.

The Authority for Privacy Protection issues CDON AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Articles 5(1)(c), 12(6) and 12(2) of the GDPR.

Report on the supervisory matter

The procedure

The Authority for Privacy Protection (IMY) has initiated supervision regarding CDON AB (CDON or the company) due to seven complaints. The complaints have been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainants have lodged their complaints (Finland and Denmark) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of complaints relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR.

Postal address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail:
imy@imy.se
Phone:
08-657 61 00

¹ Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The supervisory authorities concerned have been the data protection authorities in Denmark, Norway and Finland.

Complaints

Summary of the complaints

In conclusion, the following general information can be found from the complaints. The complainants have requested the erasure of their personal data. The company has replied that a request can only be processed if the data subjects submits information about the date of birth, address, customer number, information about latest purchases such as order number and information on payment methods including the last four digits of the credit card number in case of card payment. Several of the complainants argue that their purchases were made so long time ago that they were unable to find all the information requested. The complainants dispute that all the information requested is necessary in order to confirm their identity and to handle their requests.

What the complainant and CDON have stated in the respective complaint

Complaint 1 (Finland with national registration number [REDACTED])

On 28 May 2018, the complainant submitted a request for the erasure of his personal data. The company has replied that a request can only be processed if the data subject submits the date of birth, address, customer number, order number, payment method for the latest order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

In conclusion, the complainant states that she cannot remember or find the information requested by the company since the order was made 5-10 years ago.

Complaint 2 (Finland with national registration number [REDACTED])

On 25 May 2018, the complainant contacted CDON and requested the erasure of its customer data. The company has replied that they require information on the date of birth, customer number, order number and payment method for the latest order. The complainant states that it is unreasonable to have to answer these questions in order to be able to exercise its rights. The complainant does not retain the information requested by the company and has used the e-mail linked to the customer account for the request for erasure.

Complaint 3 (Finland with national registration number [REDACTED])

On 31 May 2018, the complainant contacted the Finnish Data Protection Authority after requesting access to and erasure of the complainant's data at the company. On 29 May 2018, CDON replied to the complainant's request that, in order to verify the complainant as a customer they need, their address, customer number, order number from the last order, payment method for the last order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

The complainant states that it was a long time ago something was purchased from CDON and that he or she does not have the information the company requires. It is

further stated that the company does not seem to delete the data without receiving answers to its detailed questions in the event of a request for erasure.

Complaint 4 (Finland with national registration number [REDACTED])

On 31 May 2018, the complainant applied to the Finnish Data Protection Authority after requesting erasure from the company. It was 5-10 years ago since the complainant ordered something from CDON. In order to be able to delete their data, the complainant needs to send data from his purchase that is from several years back in time to the company. The complainant also needs to provide personal data that was not previously needed to make a purchase in the first place. The company informed in its reply to the complainant that there is a right to access and erasure of personal data but that the company as a controller has the right to retain certain personal data for accounting purposes. In order to comply with a request, for security reasons, the company needs to be informed of the complainant's date of birth, address, customer number, order number from the last order, payment method for the latest order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

The company states that it is not in a position to verify the date on which the complaint was lodged with the company or the date on which it requested additional information from the complainant. Since the complainant have not been active customer of CDON for the last two to five years, CDON also confirms that the complainants' personal data were removed from CDON's system and that no information on the complainant remains.

Complaint 5 (Finland with national registration number [REDACTED])

The complainant has contacted the Finnish Data Protection Authority after requesting the erasure of its data at the company. The company have informed the complainant that there is a right to access and erasure of personal data but that the company has the right to retain certain personal data for accounting purposes. In order to comply with a request, for security reasons, the company needs to be informed of the complainant's date of birth, address, customer number, order number from the last order, payment method for the latest order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

The complainant does not remember when an order was placed from the company and how the purchase was paid. It's been over a year since something was ordered.

The company states that it is not in a position to verify the date on which the complaint was lodged with the company or the date on which it requested additional information from the complainant. Since the complainant have not been active customers of CDON for the last two to five years, CDON also confirms that the complainants' personal data were removed from CDON's system and that no information on the complainant remains.

Complaint 6 (Finland with national registration number [REDACTED])

The complainant lodged a complaint with the Finnish Data Protection Authority following a request for erasure from the company on 21 May 2018. The complainant

states that the company makes it difficult to exercise the right to erasure by requesting information that a customer should not be obligated to save. The process contributes to a long wait until the request of right to erasure is met. In its reply to the complainant on 29 May 2018, the company requested information on the date of birth, address, customer number and one of the following:

- Order number from the last order;
- Payment method for the last order;
- if invoice: price and reference number
- if card payment: the last four digits of the credit card number
- if direct payment: reference number and receipt

Complaint 7 (Denmark with national registration number [REDACTED])

The complainant claims to have attempted to delete his customer account online on cdon.dk by using a hyperlink <http://cdon.dk/>. The company replied to the complainant on 29 May 2018 requesting information regarding the date of birth, address, customer number, order number from the last order, payment method for the last order including the last four digits of the credit card number. The complainant states, inter alia, that the company requires more information when exercising the right to erasure than in the creation of the customer account. The complainant used the same e-mail address for the request for erasure as for the creation of a customer account at the company.

What CDON AB has stated

CDON AB has mainly stated the following.

Complaints

Of the complaints covered by this case, CDON has been able to identify six out of seven complainants against information in its systems. As regards to those six complainants, CDON is the controller of the processing of personal data to which the complaints relate.²

When the company received the requests for erasure, it contained the complainants' name and e-mail address. However, CDON considers that only those two data are not sufficient to ensure the identity of the complainant. CDON has therefore requested additional information from all complainants pursuant to Article 12(6). In addition to their name and e-mail address, the complainants were required to provide the following information in order to ensure their identity:

- Date of birth;
- Address of civil status;
- Customer number;
- The order number of the latest order; and
- Payment method for last order.

In addition, the complainants had to provide the following information on payment methods:

- In the case of invoice purchases: price and reference number;
- In case of card payment: the last four digits of the card;
- In case of direct payment: reference or invoice number.

² CDON has not been able to identify complainant in complaint [REDACTED] (complaint 5). However the company has stated that it is possible that the complainant has had a customer relationship with CDON under a different email address than indicated in the complaints sent to the supervisory authority which cannot be verified.

Current routine

In this context, CDON deems, receiving complaints concerning difficulties for data subjects in exercising their rights under the GDPR to be a matter of concern and has therefore continuously worked to improve its identification procedures when exercising the right of erasure and access. Since 2018, when the complaints were received, the identification process has been reviewed and clarified. Over the years, CDON has worked to improve handling and ensuring a simple and secure process for requests for erasure. Customers who wish to request erasure or access are directed to contact the customer service at kunddata@cdon.com. When a data subject contacts the company with a request for erasure, the company informs the data subject that the data subject's e-mail will shortly be unsubscribed from the CDON newsletter (if such subscription is activated). In order to have their account deleted, CDON currently asks the customer to answer two security questions (one each from category 1 and 2) in order for CDON to ensure that the person who contacted the company is correctly registered. Data subjects may choose to answer one question from the respective security category of questions provided by CDON. This means that data subjects need to answer only one of the following category 1 security questions. According to the verification questions in category 1, customers must state the date of birth³, the registered address or the customer number on CDON.com. Thereafter, data subjects need to answer only one of the following category 2 security questions. The control questions in category 2 are connected to recent orders where the customer either enters the order number or, depending on the payment method, enters one of the following information: when invoiced; amount and OCR number, in case of card payment: the last four digits on the card and in the case of direct payment; transaction ID or invoice ID.

In the event that a customer does not want or is unable to answer the security questions requested, the data subject is also offered the opportunity to contact customer service to follow-up and investigate an alternative security method to verify the data subject's identity. CDON considers it necessary to provide at least two additional information in addition to the name and email address of customers according to the company's new routine in order to be able to verify with sufficient certainty that it is the right person making a request. CDON's procedure for the identification and verification of the data subject does not involve the collection of new information about the data subject. CDON only requests to have two different data verified against the data that CDON already processes about the data subject with a legal basis in order to verify the identity of the data subject.

The company's retention period

CDON has stated that they have a separate retention period for e-mail and another retention period for personal data. CDON's retention period for e-mail means that all emails received to CDON's customer data box i.e. kunddata@cdon.com to which customers are referred to if they have requests for erasure or access, will be deleted after 14 months from the date of receipt at CDON. The erasure of customer profiles on CDON is currently carried out based on consumer law obligations in different countries, for example after three years in Sweden. CDON therefore confirms that all complainants have been deleted at CDON.

³ Since 22 January 2021, CDON only collects birth numbers (if data subjects choose to add that information in category 1) and not the full personal identity number.

Justification of the decision

Applicable provisions, etc.

In order for personal data processing to comply with the GDPR, the processing must inter alia comply with the requirements regarding the principles of processing of personal data set out in Article 5 of the GDPR, including the principle of data minimisation (Article 5(1)(c) and the principle of accountability (Article 5(2).

According to Article 5(1)(c) GDPR, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

According to Article 11(2) where in the cases referred to in paragraph 1 of this article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling the identification.

Article 12(2) requires the controller to facilitate the exercise of the data subject's rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

Article 12(6) provides that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject. The European Data Protection Board (EDPB) Guidelines 01/2022 on the right of access state as follows.

As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.⁴

The controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data, and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32 GDPR, including for instance a secure channel for the data subjects to provide additional information. The method used for authentication should be relevant, appropriate, proportionate and respect the data minimisation principle. If the controller

⁴ EDPB Guidelines 01/2022 on data subject rights - Right of access Version 2.0 Adopted on 28 March 2023, paragraph 70.

imposes measures aimed at authentifying the data subject which are burdensome, it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).⁵

Assessment of the Authority for Privacy Protection (IMY)

Complaints

Pursuant to Article 57(1)(f) of the GDPR, IMY shall deal with complaints and, where appropriate, investigate the subject matter of the complaint. The case includes seven complaints. IMY has requested CDON to comment on the information it has requested, the need for each individual information, the date on which the request for erasure was received in the respective complaints, the date on which it requested additional information to confirm the identity of the respective complaints and whether the complainant contacted the company after 25 May 2018.

Complaints 4 (Finland with national registration number [REDACTED]) and 5 (Finland with national registration number [REDACTED]) do not indicate the date on which the complainant made a request for erasure with the company or when the company requested the additional information. The company has stated that it has deleted the complainant's personal data in these two individual complaints in accordance with its retention period procedure and cannot verify the date on which the request in the respective complaint was received or handled. IMY finds no reason to doubt that CDON was unable to find any information about the complainant and its request for erasure. Several years have passed since the complaints were submitted to the Finnish Data Protection Authority.

IMY notes that it is not possible to draw any conclusive conclusions from what has been done in the two complainants' case on the basis of what has been possible to investigate in the complaints. In particular, in view of the fact that the complainants' requests relate to the time close to when the GDPR entered into force, it has not been possible to ascertain whether those two complaints fall within the scope of the GDPR. CDON has further confirmed that no personal data relating to these two complainants are no longer being processed by the company. Against this background, IMY considers that the substance of the complaint is investigated to the extent appropriate under Article 57(1)(f) of the GDPR. IMY therefore finds no reason to investigate these two complaints further.

Consequently, IMY has, on the basis of the remaining five complaints in the case, examined the company's conduct in these individual cases. IMY has also examined whether the company's current routine is compatible with the General Data Protection Regulation.

General starting points

It can be concluded that, in order to identify a data subject, the controller may request additional information that is necessary, where the controller has reasonable grounds to doubt the identity of the person making the request.

⁵ EDPB, Guidelines 01/2022, paragraph 71.

The GDPR does not explicitly regulate what data may be requested or how the additional information is to be collected. The controller must carry out a proportionality assessment in order to determine what is appropriate with regard to the Regulation's requirements, *inter alia*, for security reason, but also in the light of the requirement in Article 12(2) of the GDPR, according to which the controller shall facilitate the exercise of the data subject's rights. IMY finds that, requiring data on general basis for identification purposes irrespective of whether the data is necessary as described in Article 12(6) is contrary to both this provision and also to the principle of data minimisation in Article 5(1)(c).

As follows from the wording of the above-mentioned provisions which is also confirmed by the EDPB Guidelines 01/2022 on the right of access, the controller must carry out a proportionality assessment and be able to justify the verification method used. In order to avoid excessive data collection, a request for additional information must be proportionate to the type of data being processed and the damage that it may occur. This is also confirmed by the guidelines.⁶

Has there been an infringement of the GDPR in regards to what has been raised in the complaints in this case?

The question is whether the information required by the company to comply with the requests in the individual cases where the GDPR applies (i.e. complaints 1-3 and 6-7) has been necessary to identify the respective complainant and thus in accordance with the GDPR. The information that the company has required, in addition to name and e-mail, has been the date of birth, the civil registration address, customer number, order number and payment method for the latest order, and, depending on the payment method, price and reference number for invoice payment, the card's last four digits for card payment or reference or invoice number in case of direct payment.

The company has been given the opportunity to justify if all of the required personal data requested was necessary in order to identify the complaints in the individual cases. Without further explaining the necessity of the information requested, the company has stated to IMY that it was not enough with only name and e-mail to identify the complaints and verify that it was the correct person making the request. IMY finds that, the company's statement does not provide sufficient evidence to conclude that all of the requested data at issue were necessary to identify the data subjects in accordance with Article 12(6) and the principle of data minimisation in Article 5(1)(c). As a data controller CDON shall be able to demonstrate that the processing is carried out in accordance with the GDPR (Article 5(2)). IMY believes that CDON has not done so. IMY therefore notes that CDON AB processed personal data in breach of Article 5(1)(c) and 12(6) of the General Data Protection Regulation.

In the present case, the complainants had to provide a relatively large number of personal data in order to exercise their right to erasure, including the order number and the price of the latest order and the reference number for invoice purchases together with additional information. In some cases, it has been a long time since the complainants have purchased anything on CDON. This means that the complainants have not been able to exercise their right to erasure under Article 17 without having to make an effort to search for a large amount of information and in some cases also information that is quite old. Thus, by using such a burdensome verification method in the handling of request for erasure without justification, the company has not facilitated

⁶ EDPB, Guidelines 01/2022, General considerations on the assessment of the data subject's request, page 2-3.

the exercise of data subjects' rights as required by Article 12(2). CDON AB has thus processed personal data in breach of Article 12(2) of the GDPR.

Is the company's current routine compatible with the GDPR?

The investigation shows that the company has continuously reviewed its procedures for handling requests for erasure since 2018, when all the complaints in the case were received. The general routine examined are those in force from 22 January 2021 until the date of IMY's decision in the case in question.

In order to ensure the identity of the data subject requesting erasure, the data subject now needs to answer two questions (one question in category 1 and one question in category 2) such as date of birth and order number. Since 22 January 2021 the data subjects does not need to provide a personal identity number but only the date of birth if the data subject chooses to add that information in category 1. It is not new personal data that is requested to confirm the identity of the data subject, but two different data to compare it with data that the company already is processing regarding the data subject in order to verify the data subject. The fact that CDON verifies the identity of the data subject before erasure of personal data is also a protection for the data subject who should not have his or her personal data deleted by mistake. The company also offers an alternative way for the data subject who cannot or does not want to answer the security questions, namely to contact the customer service to find another way to verify the identity of the data subject. Therefore, a customer who has not placed an order, there is the option to contact customer service instead.

Against this background, IMY considers that CDON's existing routine is not disproportionate and therefore not in breach of the GDPR, provided that it collects only the data contained in the routine in situations where there is reason to doubt the identity of the data subject and that only the data necessary to identify the data subject is requested.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The investigation in question covers CDON AB's handling of five individual complainants' requests in relation to the respective complaints.

The company has taken measures to make it easier for data subjects to exercise their rights in accordance with the GDPR and changed their procedures to ensure that they are compliant with the GDPR. Some measures had already been taken before the start of this supervisory case. Furthermore, the infringements found occurred relatively

long time ago. In addition, the company has not previously acted in breach of the GDPR.

Against this background, IMY considers that this is a minor infringement within the meaning of recital 148 and that CDON AB must be given a reprimand in accordance with Article 58(2)(b) of the GDPR for the infringements found.

This decision has been made by [REDACTED], Head of Unit, after presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.



ROMÂNIA
AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL



Bld.Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poștal 010336, București ; Tel: +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

CONTROL DEPARTMENT

No. _____ / _____

Decision

Following the investigation performed at Bergenbier SA

The National Supervisory Authority for Personal Data Protection, with the headquarters in 28-30 General Gheorghe Magheru Blvd. District 1, post code 010336, Bucharest, legally represented by [REDACTED] [REDACTED], president, **issues this decision against BERGENBIER SA**, with the headquarters in 9-9A Dimitrie Pompei Street, Building 20, 1st Floor, District 1, Bucharest, Romania, registered with the Trade Registry under no. J40/209/1999, sole registration code 6608725, legally represented by Mr./Mrs. [REDACTED] [REDACTED], as director

Considering the following:

I. Personal data security breach notifications received based on Article 33

Molson Coors Global Business Services SRL notified a personal data security breach, by filling in the form regarding the breach of the personal data security provided under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), registered at the National Supervisory Authority for Personal Data Processing under no. 4618/12.03.2021.

Bergenbier SA notified a personal data security breach, by filling in the form regarding the breach of the personal data security provided under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), registered at the National Supervisory Authority for Personal Data Processing under no. 9923/28.05.2021.

Considering the above, ANSPDCP started an investigation at Bergenbier SA considering the mentions from the notification form no. 9923/28.05.2021, according to which „In Romania, Molson Coors activates through 2 entities – Bergenbier SA and Molson Coors Global Business Services SRL. The internal investigation of the Molson Coors Group showed that the controller is Bergenbier SA (and not *Molson Coors Global Business Services S.R.L.*)“.

Through the address no. 10624/08.06.2021, ANSPDCP requested additional information from **Bergenbier SA**, in order to identify the lead supervisory authority competent to handle the security breach notified through the forms no. 4618/12.03.2021 and no. 9923/28.05.2021.

Bergenbier SA responded through the address no. 11360/22.06.2021, as it follows: "... at the level of Molson Coors Beverage Company an official designation of a representative in the Union, based on Article 3 paragraph 2 and Article 27 of the GDPR, was not performed. In this case, our internal investigation

Notă Informare RGPD

https://www.dataprotection.ro/?page=Informare_protectia_datelor_conf_GDPR

showed that the personal data controller responsible to notify the incident in the European Union is Bergenbier SA – an entity from the European Union.”

Following the response provided through address no. 11360 from 22.06.2021, the National Supervisory Authority for Personal Data Processing (hereinafter, referred to as "ANSPDCP") acted as lead supervisory authority (LSA) in this case, considering that this company has its main establishment in Romania, by introducing within the application "Internal Market Information System" a notification according to Article 56 in order to inform the supervisory authorities from the other European Union Member States, registered under no. 428112.

We hereby present a resume of the security incident and of the results of the investigation performed by ANSPDCP in this case.

II. Description of the case:

According to the mentions from the notification form no. 9923/28.05.2021, on 9th of March 2021, time 12:00, it was identified that the global network and systems of the Molson Coors Group were subject of a cyber-attack. The internal investigation showed that one or several cyber attackers has/have gained access to the Molson Coors Group systems and installed "malware" type computer programs through the network, existing clues that certain information were copied by the attacker(s). Also, the investigation showed that the cyber-attack affected a server located in Ploiești, used by the controller in order to store information.

As part of the Molson Coors Group (as defined below) the controller benefits from a complete range of controls for detecting the cyber threats and of prevention measures. This range includes, but is not limited, to the following:

- a computer program "firewall" type (network perimeter firewall) against the unwanted traffic, dangerous codes and intrusion attempts;
- the use of the "proxy" type server that acts as a gate between the business activity and internet and that verifies, before transmission, the communications;
- the use of a detection "endpoint" and of an antivirus computer program in order to monitor the access points (such as the laptops of the users) and to mitigate the cyber threats;
- a security team allocated 24/7 that monitors the threats received via e-mail and the "phishing" attacks and that is responsible for monitoring the antivirus brackets and alerts and acts in case of incidents;
- a special antivirus protection plan;
- a computer program Advanced Threat Protection type used for the detection, investigation and counteraction of the cyber-attacks on the network;
- A computer program Endpoint Protection Client type for the Windows servers;
- a software application that detects and responds to threats, installed by a security services provider in order to detect, investigate and combat the threats on the access points and network;
- the handling, monitoring and reporting of the journal files;
- intrusions detection systems;
- segmentation within the network in order to separate the "legacy" type network from the virtual networks;

- outsourced security controls;
- vulnerabilities detection;
- active vulnerabilities scanning.

The type of the personal data security breach is: availability and confidentiality.

The nature and content of the personal data envisaged: personal data of the current and former employees, as well as of other data subjects (first name and last name, date of employment, PIN, series and number of the identity card, date of birth, bank account, ID/employee mark, number of the credit/debit card, the position held and others).

A number of 6334 natural data subjects was affected.

The controller benefited from a series of organisational and technical measures for the mitigation of the risks generated by this security breach, respectively:

From organisational perspective:

- The employment of external experts, in order to assist the controller with the implementation of the mitigation measures and within the investigation;
- the activation of a response plan to the incident;
- The forming of a working group composed of internal decision factors and external experts, to address both the organisational as well as technical aspects of the security incident, including the analysis of the high risk for the rights and freedoms of the affected data subjects.

From technical perspective:

- Immediately after the incident, they disconnected any external connexions including the VPN access type and Virtual Desktop access in order to allow the adequate cleaning of the systems and the remedy of any problems;
- They improved the authentication systems for the IT systems dedicated to the employees and providers;
- They added additional programs for the detection and prevention of any unauthorized access on the computers, laptops and mobile devices;
- They used extended software applications in order to detect and respond to the threats and programmes that continuously verify the systems in order to detect any suspicious activity and to stop the potential threats.
- They informed that natural data subjects affected by the incident by the e-mail addresses (for the former employees) and through the web page www.bergenbier.ro, section "GDPR Alert" (for former employees and third parties).

According to those declared through the security breach notification form submitted, it resulted that also natural data subjects from other member states of the European Union were affected such as: Hungary (427 persons), Czech Republic (677 persons), Slovakia (44 persons) and Croatia (658 persons).

In Romania an estimated number of 2636 natural data subjects were affected.

III. Handling steps taken by ANSPDCP

Through the address no. 10624/08.06.2021, ANSPDCP requested additional information from Bergenbier SA, that responded through letter no. 11360/22.06.2021 as it follows:

Q1: "considering that the company Bergenbier SA is part of the Molson Coors Beverage Company that has its headquarters in United States of America, those declared under points 16 and 17 from the notification form, as well as those mentioned above, please inform us if Molson Coors Beverage Company has designated a representative in the European Union and what this is, in order to identify the lead supervisory authority."

A1: *Molson Coors Beverage Company is a multinational beverages and beer company with two executive offices in Golden, Colorado and Montreal, Quebec, with activity in various states, including Romania.*

At the level of the Molson Coors Beverage Company an official designation of a representative in the Union, based on the Articles 3 paragraph (2) and 27, was not performed. In this case, our internal investigation showed that the personal data controller competent to notify the incident in the European Union (as defined below) is Bergenbier SA – an entity from the European Union.

Within Molson Coors a global Ethics and Compliance team, responsible with the support of the development and implementation of the practices that facilitates the compliance with the applicable legislation and policies of the Molson Coors Group, acts. For the successful fulfilment of the role held, the team is composed of members from the United States of America and Europe that are responsible, among others and each in relation to its own geographical jurisdiction, with the monitoring of the compliance with the applicable legislation in the field of the personal data protection within the Molson Coors Group.

We underline that the members of the global Ethics & Compliance team are closely handling the ensurance of the compliance with the provisions of the legislation applicable in the personal data field and are supported in this effort by the persons having competences from different levels within the organisation and in different territories around the world.

Q2: "please mention the residence states of the data subjects, as well as the number of data subjects affected detailed for each European Union member state /third party state, as well as if other supervisory authorities have been notified in relation to the security incident that took place at the level of Molson Coors Beverage Company";

R2: *Our client cannot perform an identification of the residence state of the data subjects due to the lack of the adequate technical and logistic means in order to perform this investigation. However, based on the information available at this moment, our client can provide a list with the estimated numbers of the data subjects broken down on each European Union member state/third party state. Therefore, please find attached to this answer a list containing the estimated number of the data subjects detailed on each of the European Union member state/third party states, in certified true copy (Annex 1).*

We underline that within 72 hours from the incident, as it was indicated within the notification registered within the General Registry of ANSPDCP under no. 4618/12.03.2021 and detailed within the completion of the notification registered within the General Registry of ANSPDCP under no. 9923/28.05.2021 ("the Incident"), the Molson Coors Group, through the affiliated entities, notified the relevant supervisory authorities.

More precise, in Romania, Molson Coors Global Business Services SRL notified ANSPDCP as lead supervisory authority in relation to the processing within the European Union. This notification was registered within the General Registry of ANSPDCP under no. 4618/12.03.2021. In Great Britain, Molson Coors Brewing Company (UK) Limited notified Information Commissioner's Office ("ICO"), and in Canada, Molson Canada 2005 notified the Privacy Commissioner of Canada.

Following the internal investigation, the support of the external experts contracting for assisting the remedy and investigation process and of the correspondence with different supervisory authorities, the need to submit additional notifications or to provide clarifications resulted.

Therefore, in Romania, Bergenbier SA submitted a completion to the notification registered within the General Registry of ANSPDCP under no. 4618/12.03.2021, considering the fact that the internal investigation revealed that Bergenbier SA is, actually, the controller of the personal data competent to notify the Incident within the European Union. This completion of the notification was registered within the General Registry of ANSPDCP under no. 9923/28.05.2021.

In Great Britain, ICO requested additional information regarding the incident and the progress of the internal investigation, an update of the notification being correspondingly submitted. ICO closed the investigation and confirmed that no other measures will be taken.

In Canada, an additional notification and a model of individual information notice were submitted to Privacy Commissioner of Canada.

Country	Estimated number of data subjects
Romania	2636
Serbia	770
Hungary	427
Bosnia and Herzegovina	84
Bulgaria	748
Montenegro	242
Czech Republic	677
Slovakia	44
Croatia	658
Great Britain	2
Not determined	46

Subsequently, through address no. 14822/02.09.2022 ANSPDCP requested additional information to Bergenbier SA, that responded through address no. 15392/13.09.2022 as it follows:

Q1: The investigation report of the incident performed with the support of the experts

A2: *The incident investigation report performed with the support of the experts, we attach to this answer the incident investigation report performed by Securityworks Inc. in the English version (certified true copy – Annex I.A) and translated into Romanian (Annex I.B.) to the extent you consider appropriate, at your request, we can also make available a legalized translation in Romanian of the incident investigation report.*

Q2: Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide the **evaluation procedure/methodology regarding the risk for the persons' rights and freedoms;**

A2: Considering the provisions of Article 24 and Recitals 75 and 76 of Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide the evaluation procedure/methodology

regarding the risk for the persons' rights and freedoms, we mention that the methodology used by our Client involved the following steps:

Step 1: The identification of the existence or not of the personal data within the incident

Step 2: Establishing the categories of personal data affected

Among the personal data affected are:

- *First name and last name, PIN, number and series of the identification card, number of the banking account, number of the credit/debit card and/or*
- *Address and/or date of birth and/or the position held at the previous work place and/or date of employment*
- *Among the personal data affected there are no data from the category of special data (as provided under Article 9 from the General Data Protection Regulation)*

Step 3: The identification (as much as possible) of the third persons that could have access to the personal data affected by the incident;

- *The investigation showed that the cyber attacker/attackers had unauthorized access to the personal data identified at Step 2 above;*

Step 4: the evaluation of the general context of the incident

- *The identification of other details related to the incident, the type of unauthorized access, the working method of the cyber attacker/attackers, and others*

Step 5: the evaluation of the risks and the review and update of the corresponding measures

- *The analysis of the categories of personal data and of the context of the unauthorized processing, as well as of the probability of any risk on the data subjects' rights and freedoms and the adopting of additional measures in order to increase the protection of the data subjects (please see the measures of the Human Resources Operations Department detailed below).*

Q3: Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide us an evaluation regarding the risks for the persons' rights and freedoms that contain inclusively the framing within a risk degree (low, medium, high)

A3: Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, by reference to point 11 from the notification "possible consequences and adverse effects (risks) for the natural data subjects", we hereby request you to provide us an evaluation regarding the risks for the persons' rights and freedoms that contain inclusively the framing within a risk degree (low, medium, high), our Client performed an evaluation based on the following criteria:

The potential impact that the incident could have had, generally, on the life of the data subjects and if the incident could have affected them in any manner:

- *The following questions were of interest for our Client:*

Can the incident create an unsecure situation in which the affected data subject would be?

Can the affected data subjects lose money or the workplace following this incident?

Can the incident affect the health or the good living of the affected data subjects?

The attempt to identify the impact helped our Client to identify the measures necessary to be taken in order to limit the negative effects of it and to protect the data subjects from subsequent injuries.

The categories of personal data affected

- *These were identified according to Step 2 detailed within the methodology from above.*

The manner in which the unauthorized access could affect the data subjects; in other words, how could the data be used?

Considering the methodology applied and the criteria above, our Client paid more attention to the following aspects:

- *No special categories of personal data were accessed;*
- *Although there have been accessed some financial personal data or data from the identity card, the probability for this access to lead to a financial loss and/or fraud of the identity was classified as medium to low, considering that the financial institutions frequently have advanced security measures, such as multiple authentications, in order to verify and, thus, to prevent the identity frauds or other similar incidents.*

However, our Client decided, out of prudence, to qualify this incident as having a high risk for the affected data subjects and, therefore, to notify the data subjects, as we also showed within the completion to the notification registered within the General Registry of ANSPDCP under no. 9923/28.05.2021, and to adopt the indicated additional technical and organisational measures.

Q4: possible additional technical and organisational measures adopted, by reference to Article 32 GDPR, following the investigation performed

A4: the possible additional technical and organisational measures adopted, by reference to Article 32 GDPR, following the investigation performed, we mention the following aspects:

- At technical level, the IT security of the Molson Coors Group (that our Client is part of) is centrally governed and is part of the global network. As a response to this incident, based on the cyber security plan, several amendments were implemented both at technical and processes level. A company specialised in response to information security related incidents services was contracted (Securityworks Inc, as we showed in point 1 above) for the assistance related to the response and recovery process. Therefore, several remediation actions needed to be adopted following the activity of the cyber attacker/attackers, as is mentioned in the report attached to this response. Therefore, the additional measures include:

Multi-factor authentication system for all the remote access methods

The limitation of the number of users that have management rights within the Microsoft Active Directory system and the implementation of a management system for the privileged access (IBM Secret Server) in order to monitor the access data corresponding to the special critic accounts. Our Client included a control for review of the rights and access data within the list of the compliance controls in order to ensure that these rights and access data are periodically, quarterly revised;

The implementation of a computer program for the detection and counter-attack of the information attacks, program acquired from the Security Services Provider (MSSP) (Secureworks), on all the working stations of the users and on the Windows and Linux servers from the data centres and the beer factories connected in the same network; the update of the type of services offered to MSSP in order to move from outsourced personnel services to services for the management of the detection and counter-attack of the

information attacks. Also, the number of employees from the Security Operations Centre was increased. These actions were finalized in July 2021, considering the time necessary to make the transition to this new type of services and to employ additional human resources

Performing an action to renew all passwords, including the Kerberos tickets;

The update of the passwords' policies by amending the length requirement to a minimum of 12 characters and at the same time the increase of the size of the validity period of the password from 90 days to 365 days

Adding a computer program for the detection of the phishing attempts and their automatic rejection, in addition to the computer program

Microsoft Advanced Threat Protection, for a better detection of the phishing e-mails

The blocking of the access to certain websites that allow the sharing of data as well as of the data sharing applications, by using different computer programs, such as Zscaler Internet Access (Internet firewall);

The update of all the working stations from Windows 7 to Windows 10

The installation of the computer programs Microsoft Azure Information Protection and Microsoft Identity Protection, as well as the enhancement of the data loss detection and prevention mechanism made available by the computer program Microsoft Office 365;

The replacement of the existing solution for VPN with a new one, „reverse proxy security type, named Zscaler Private Access, that allows a „zero-trust" type approach for network access. This new solution continues to use the authentication with multiple factors for remote access

The launch of a global training program for the awareness of the security risks, program named CyberSIP.

The implementation of additional options for archiving and recovery of the data and the inclusion of a data copy option that does not involve the connection to the network.

-At organizational level, at the beginning of January 2022, the Human Resources Operations Department implemented additional measures to ensure a high level of employees' data protection, in this respect the Human Resources Operations Department was notified in relation to the need to comply with the following additional rules:

The protection with password of the documents: any personnel file containing personal data will be protected with password, The provision of the documents protected by password will be performed via a different e-mail from the e-mail through which the password will be communicated;

The control of the provision: any personnel file that contains personal data will be transferred solely to the department employees responsible with/with attributions (access based on the position);

The access to internal platforms: the access on the Sal wages platform and on the platform named People Central will be performed solely using user name and password (in addition, for the access on the SAL wages platform, a special license is necessary), and the level of access is granted depending on the position held and the responsibilities/job description (access based on positions)

The verification of the access: the Operations Manager verifies the audit report issued by the SAL wages platform in order to ensure that the access of the employees is according to those described above.

Q5: the last audit report regarding the certification according to the standard *ISO/IEC 27001:2013*, in case that at the company level a certified management level for the security of information is implemented

A5: the last audit report regarding the certification according to the standard *ISO/IEC 27001:2013, in case that at the company level a certified management level for the security of information is implemented, our Client does not have the ISO/IEC 27001:2013 standard implemented, but it has to be mentioned that its informatic security program is based on the Cyber Security NIST Framework.*

IV. The information of the concerned supervisory authorities within IMI

On 12.08.2022, the other supervisory authorities were informed, through the IMI application, within a procedure for identification of LSA and CSA (based on Article 56 GDPR), about the security incident, as well as regarding the intention of our institution to act as lead supervisory authority, registered under no. 428112, the deadline being 13.11.2022.

Until the date of this report, the following supervisory authorities declared as CSA:

- The Supervisory Authority from Netherlands (with the mention that "based on the information we cannot decide if the data subjects from Netherlands were affected by this incident. However, we will consider ourselves CSA in order to be sure")
- The Supervisory Authority from Poland (with the mention "In case the data subjects that live in Poland are affected, we want to be considered CSA")
- The Authority from Bulgaria;
- The Authority from Hungary;
- The Authority from Berlin, Germany (with the mention "In case the data subjects residing in Berlin are affected, we want to be considered CSA")

On 20.03.2023, through the IMI application, ANSPDCP informed the supervisory authorities from the EU states, which declared themselves "concerned supervisory authority", within the consultation procedures (based on art. 60 para. (7) of the RGPD), regarding the draft decision to be adopted following the investigation carried out.

The response deadline was set in IMI until 11.04.2023.

As a result of the verification carried out in the IMI application, on 12.04.2023, it was found that no comments/objections were made regarding the draft Decision.

V. Conclusions:

From the investigation performed by ANSPDCP through the address no. 10624/08.06.2021 and nr.14822/02.09.2022, and from the Bergenbier SA answers no. 11360/22.06.2021 and no. 15392/13.09.2022, the following resulted:

- The security incident consisted of the unauthorized access of the personal data of the employees/former employees/other data subjects from the Molson Coors Group entities, data subjects from several Member States being affected;
- The personal data affected:

- first name and last name, PIN, number and series of identity card, number of bank account, number of the credit/debit card and/or
 - address and/or date of birth and/or the position held at the previous work place and/or the date of employment
- The investigation showed that no special categories of personal data were unauthorized accessed.
- As a response to this incident, based on the cyber security plan, the controller implemented several amendments both at technical and processes level. A company specialized in informational security response services was contracted (Securityworks Inc) for the assistance related to the response and recovery process.
- Subsequently to the security incident, additional technical and organizational measures were adopted, finalized in July 2021. These include:
 - Multi-factor authentication system for all the remote access methods
 - The limitation of the number of users that have management rights within the Microsoft Active Directory system and the implementation of a management system for the privileged access (IBM Secret Server) in order to monitor the access data corresponding to the special critic accounts
 - A control for review of the access rights and date within the list of the conformity controls in order to ensure that these rights and access data are periodically, quarterly re-certified
 - The implementation of a computer program for the detection and counter-attack of the information attacks on the working stations of the users and on all the Windows and Linux servers from the data centres and beer factories connected in the same network; the update of the type of services offered by MSSP to pass from the external personnel services to services for management of the detection and counter-attack of the information attacks
 - The increase of the number of employees from the Security Operations Centre.
- Performing an action to renew all passwords, including the Kerberos tickets;
- The update of the passwords' policies by amending the length requirement to a minimum of 12 characters
- Adding a computer program for the detection of the phishing attempts and their automatic rejection, in addition to the computer program Microsoft Advanced Threat Protection, for a better detection of the phishing type e-mails;
- The blocking of the access to certain websites that allow the sharing of data as well as of the data sharing applications, by using different computer programs, such as Zscaler Internet Access (Internet firewall);
- The update of all the working stations from Windows 7 to Windows 10;
- The installation of the computer programs Microsoft Azure Information Protection and Microsoft Identity Protection, as well as the enhancement of the data loss detection and prevention mechanism made available by the computer program Microsoft Office 365;

- The replacement of the existing solution for VPN with a new one, „reverse proxy security type, named Zscaler Private Access, that allows a „zero-trust" type approach for network access.
- The implementation of additional options for archiving and recovery of the data and the inclusion of a data copy option that does not involve the connection to the network.
- The protection through password of the documents; provisions control; access to internal platforms by using user name and password
- Bergenbier SA informed the data subjects affected by the incident were informed as it follows: the current employees were informed by e-mail and the information of the former employees and/or third parties was performed on the website www.bergenbiersa.ro, section GDPR Alert;
- following the introduction of the case within the IMI application the following member states declared as being concerned supervisory authorities: Netherlands, Poland, Bulgaria, Hungary and Germany
- Following the investigation procedures performed it was found that a number of 6334 data subjects were affected from the following states: Romania, Serbia, Hungary, Bosnia și Herzegovina, Bulgaria, Montenegro, Czech Republic, Slovakia, Croatia, Great Britain;
- From the verifications performed until the conclusion of this report,, it was found that no complaints were submitted by the security incident notified by Bergenbier SA.

VI. Analysis according to the Article 83 GDPR criteria

The conclusions resulting following the analysis of the security incident according to the Article 83 GDPR criteria:

- a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
 - 6334 data subjects affected (employees/former employees/third parties)
 - The systems and global network of the Molson Coors Group were subject to a cyber-attack following which one or several cyber attackers has/have gained access to the Molson Coors Group systems and installed malware type computer programs through the network
 - The incident took place in March 2021, the additional technical and organizational measures, implemented by the controller for the remedy of the incident being finalized in July 2021
 - No complaints were submitted by the persons envisaged by the security incident notified by Bergenbier SA, therefore no damages incurred by them were able to be identified
- b) the intentional or negligent character of the infringement;
 - malware type cyber-attack
- c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
 - the data subjects affected by the incident were informed as it follows: the current employees were informed by e-mail and the information of the former employees and/or third parties was performed on the website www.bergenbiersa.ro, section GDPR Alert;
 - an evaluation regarding the risk for the data subjects' rights and freedoms was performed
 - subsequent to the security incident additional technical and organisational measures were adopted
- d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
 - the informational security program of the controller is based on the Cyber Security NIST Framework

- a firewall type computer program (network perimeter firewall) against the unwanted traffic, dangerous codes and intrusion attempts
 - the use of a proxy type server that acts like a gate between the business activity and Internet and that verifies, before provisions, the communications;
 - the use of a detection endpoint of an antivirus type computer program in order to monitor the access points (such as laptops of the users) and to mitigate the cyber threats
 - a security team allocated 24/7 that monitors the threats received via e-mail and the phishing type attacks and that is responsible to monitor the antivirus consoles and that alerts and acts in case of incidents
 - a special antivirus protection plan
 - an Advanced Threat Protection type computer program used for the detection, investigation and counter-attack of the cyber-attacks on the network
 - an Endpoint Protection Client type computer program for the Windows servers
 - a software application that detects and answers to the threats, installed by a security services provider for the detection, investigation and combatting the threats on the access points and on the network
 - the handling, monitoring and reporting of the journal files
 - the intrusion detection systems
 - segmentation within the network in order to separate the legacy type network from the virtual networks
 - outsourced security controls
 - vulnerabilities detection
 - scanning of active vulnerabilities
- e) any relevant previous infringements by the controller or processor;
- no previous breaches were identified
- f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- the controller notified the security incident within the term provided by GDPR and communicated to ANSPDCP all the information requested within the investigation performed
- g) the categories of personal data affected by the infringement;
- first name and last name, PIN, number and series of identity card, number of bank account, number of the credit/debit card and/or
 - address and/or date of birth and/or the position held at the previous work place and/or the date of employment
 - The investigation showed that **no special categories of personal data were accessed unauthorized**
- h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- the controller **notified the security incident within the term provided by GDPR and communicated to ANSPDCP all the information requested within the investigation performed**
- i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- measures have not been applied previously
- k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

- The security incident took place following a malware type security incident and not to avoid some losses or to obtain some financial benefits directly or indirectly

Considering the findings resulted from the investigation performed at the Bergenbier SA, as well as from the analysis of the incident according to the criteria from Article 83 GDPR, we consider that in this case the application of a sanction is not required.

President,

[REDACTED]



Decision

Following the investigation performed at Dante International SA

The National Supervisory Authority for Personal Data Processing, with its headquarters in 28-30 Gen. Gheorghe Magheru Blvd., District 1, Postal code 010336, Bucharest, legally represented through [REDACTED], President, **issues this decision against Dante International SA**, with its headquarters in 148 Virtutii Road, Bucharest, District 6, Sole registration code: 14399840, registered with the Trade Registry under no. J40/372/2002, legally represented by [REDACTED] [REDACTED], as director and [REDACTED] [REDACTED], data protection officer.

Considering the following:

I. Background

Complaints received based on Article 56 and 61 of the GDPR

Through the IMI registrations under no. 179746 (based on Art. 56 from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – hereinafter referred to as „GDPR”), no. 311264 (based on Art. 61 of the GDPR), no. 311285 (based on Art. 61 of the GDPR), the National Supervisory Authority for Personal Data Processing was notified by the Data Protection Authority (DPA) from Hungary regarding the complaints submitted by three natural persons from this country against Dante International SA. DPA Hungary considered the National Supervisory Authority for Personal Data Processing (hereinafter referred to as „ANSPDCP”) as being the lead supervisory authority (LSA) in this case, considering that this company has the main headquarters in Romania. The proposal of DPA Hungary was accepted by ANSPDCP.

We hereby present a synthesis of the three complaints and of the results of the investigations performed by ANSPDCP in these cases. The detailed presentation of the ANSPDCP's steps and of the controller's replies is to be found within the minutes of findings no. 7538/19.04.2023, that will be provided in copy to Dante International SA, together with this decision.

A. [REDACTED] Case

- IMI 179746 (Art. 56)

Object of the complaint

Following the analysis of the annexes to the IMI registration, it was found that Mr. [REDACTED] has requested on 30.06.2020 the erasure of the account created on emag.hu, by having a correspondence in this respect on the address info@emag.hu. Within the response received from this address, signed by [REDACTED], clients' representative, [REDACTED] was requested to send a dated and signed request (scanned or photographed) at the address data.protection@emag.ro. [REDACTED], unsatisfied with the fact that more information than at the creation of the account is requested to him, addressed a complaint to DPA Hungary on 03.07.2020.

Conclusions:

From the investigation performed by ANSPDCP, but also from the personal data privacy policy published on the *emag* websites (*emag.ro*, *emag.hu*, *emag.bg*) it did not result that, within the procedure for the handling of the requests for the erasure of the data (or regarding the other rights provided under the GDPR), Dante International SA would impose the submission of a signed and dated request, scanned or photographed, as it was requested to [REDACTED] by the commercial department from Hungary. Thus, at the date of the complaint and of the start of the investigations, the requests of the data subjects needed to be addressed to the e-mail address data.protection@emag.hu, all the requests at the group level being automatically redirected to a unique central address of the controller, data.protection@emag.ro. In the case of the website *emag.ro*, in addition, the possibility of sending the requests also by post or courier to a physical correspondence address of Dante International S.A. was indicated.

Therefore, it cannot be concluded that, at the level of the group of companies for which Dante International SA is main establishment, in the sense of Article 4 point 16 letter a) of the GDPR, such a procedure would exist, but rather, in the case reported by [REDACTED] it represents a specific matter, at the level of the Hungarian entity (Dante International Korlátolt Felelősségi Társaság, currently with the name Extreme Digital-eMAG Korlátolt Felelősségi Társaság). The controller declared that the "case of [REDACTED] is a singular one", under the conditions that, "at the level of the Dante group, an average of 1000 requests for the exercise of personal data rights are received every month to the dedicated e-mail addresses".

However, the lack of a regular and adequate training of the group's employees by Dante International SA was found, specifically of those from Dante International Korlátolt Felelősségi Társaság (currently, Extreme Digital-eMAG Korlátolt Felelősségi Társaság), regarding the procedure to be followed for the handling of the data subjects' requests. From the controller's response it resulted that the training of the personnel from the Hungarian entity is performed at the hiring (based on a training manual), and within each entity of the group, and subsequently, in "specific situations and customized to each department". The proofs sent are referring to the communication of a document "Internal eMag policy for personal data processing", by e-mail, on 27.12.2018.

Or, according to Article 24 of the GDPR, the controller shall implement adequate technical and organisational measures, including adequate policies for data protection, in order to guarantee and be able to prove that the processing is performed in accordance with the GDPR. These policies should approach correspondingly the handling of the requests received from the data subjects and the performance of some regular training sessions of the personnel involved in the processing of personal data.

On the other hand, in cases such as that of [REDACTED], even in case a person would not address to the contact data dedicated to the exercise of the rights, but to other public contact data used for the customers' relations, the controller has the obligation to handle the requests of the data subjects (subject to their clear identification), according to the provisions of Article 12 of the GDPR, that also imposes the obligation of facilitating the exercise of the data subjects' rights based on Articles 15-22 of the GDPR. Therefore, it should be provided, for example, the possibility of redirecting, without unjustified delays, the request received on other contact data to the internal addresses from the group dedicated for the handling of the requests based on the GDPR provisions. Or, the existing procedure was imposing to the employees from the group that received such requests to guide the data subjects to contact directly the company on one of the dedicated addresses. In this respect, we reiterate the importance of a proper training of the employees/persons processing personal data under the authority of the controller, from all the entities that are part of the Dante group.

In the particular case of [REDACTED], although his request from 30.06.2020 was not immediately handled correspondingly, however after the start of the investigation by the Hungarian DPA, the controller decided to erase the data of the claimant, on 20.08.2020, within the deadline, so reasonably, within the maximum deadline of 3 months provided under Article 12 paragraph (3) of the GDPR.

We mention that Article 17 paragraph (1) letter b) of the GDPR provides the following:

"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(...)

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing."

Therefore, a violation of the provisions of Article 12 paragraph (2) and of Article 17 paragraph (1) of the GDPR regarding the controller's obligation to facilitate the exercise of data subjects and to delete personal data without undue delay is found.

Following the investigation, the controller amended its personal data privacy policy published on the *emag* websites, offering to the data subjects the possibility to send the requests based on the GDPR both on e-mail (at an address such as data.protection@emag.hu) and by post/courier at a physical address from that state.

The method of "anonymisation" used by Dante (hash MD5) is considered to present some risks for the data subjects to be reidentified (see in this respect the Opinion 05/2014 on "Anonymisation Techniques of Article 29 Working Party, WP 216, from 10th of April 2014, pages 21-22). In this respect, ANSPDCP considers that the implementation of an anonymisation method through which the risk of reidentification of the data subjects whose personal data are subject to this procedure to be prevented is necessary, according to Article 32 of the Regulation (EU) 2016/679 (for example, the SHA-256 method that generates 64 characters).

B. [REDACTED] Case

- IMI 311264 (Art. 61)

Object of the complaint

From the analysis of the documents sent, it is found that [REDACTED] claims that on the website emag.hu an account with the personal data of the client is created automatically, even when he wishes to place an order without the creation of an account, aspect considered by the Hungarian DPA as not being necessary in the steps that precede the conclusion of a contractual relationship. Also, he claimed that the box regarding the consent for receiving newsletters was pre-checked. The claimant requested the erasure of his data on 4th of July 2020 (to info@emag.hu, data.protection@emag.ro, data.protection@emag.hu), but this was not possible, given that the emag servers rejected his request as originating from an address that is not secure ([REDACTED]). The claimant argues that on 16th of July 2020 he received an answer (from info@emag.hu, [REDACTED]) within which it is brought to his knowledge that the error message was forwarded to the competent colleagues, and on 18th of July 2020 he received an answer within which again it is indicated to address to data.protection@emag.hu. On 19th of July 2020 the claimant argues that he received again an error message from the e-mail server, according to which his request was not delivered to any of the addresses. The claimant also states that a data protection officer is not available.

Conclusions:

From the investigation performed by ANSPDCP, it resulted that the procedure for the automatic creation of an account at the placement of an order on the *emag* online commerce websites is visibly brought to the knowledge of the data subjects (that do not have or do not wish to create on their own an account), on the same screen where the data related to the delivery are requested. This procedure allows the controller to handle the orders placed on the online electronic commerce platform, the personal data being those necessary for providing the confirmation of the order and for invoicing.

Also, information on the processing of the personal data and the creation of the account are provided inclusively within the documents available on the *emag* websites, in relation to the personal data protection and the general terms of use of the services of the controllers from the Dante International group.

Considering the specifics of the activity in which personal data is processed (sale-purchase of products by taking an online order, which is equivalent to concluding a distance contract), the legal provisions of Government Emergency *Ordinance no. 34/2014 regarding consumer rights in the framework of contracts concluded with professionals*, as well as for the modification and completion of some normative acts (which transposes Directive 2011/83/EU in Romania), as well as the provisions of fiscal and accounting legislation, in the case of personal data requested for invoicing are inclusively applicable. Also, the data related to the delivery address is necessary for the execution of the contract, and data such as the e-mail address or the telephone number are necessary for the confirmation of the receipt of the order and the actual delivery of the ordered product.

Therefore, it follows that such processing is legal, compared to the provisions of Article 6 paragraph (1) letters b), c) and f) of the GDPR.

Regarding the claim of the petitioner according to which the box regarding the receipt of *newsletters* was pre-checked, it was found that the petitioner did not submit evidence in this regard, and the investigation did not result in elements to confirm these claims. Thus, the controller simulated the placing of an order with the automatic creation of a new account, without any pre-checked boxes regarding receiving the *newsletter* being visible. It can still be seen on the website that, at the time of account creation, an user can tick or not if they want to receive "the best offers".

The information of the data subjects from the personal data policy on the *emag* websites was updated in relation to the transfer of data abroad.

Pursuant to Article 13 paragraph (1) letters c), e) and f) and Article 14 paragraph (1) letters c), e) and f) of the GDPR, the controller has to inform the data subjects including about the following:

- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Since, at the start of the investigation (date of ANSPDCP's letter no. 21958 of 09.12.2021, sent to Dante International SA), the information on the *emag.hu* website did not contain complete information on transfers to third countries, purposes and recipients in this context, a violation of the above provisions is found.

Regarding the automatic rejection of the requests of the claimant through which he requested the erasure of the data, the controller argues that its servers use the public lists provided by Cisco Talos Intelligence Group, maintained by a third party, on which the controller does not hold the control, and that situation was a possible one generated by the weak/bad reputation of the service *@freemail.hu* at the moment when the claimant sent those requests to Dante.

Although the controller claims that it did not receive the requests of the claimant of the 4th of July 2020 (sent to data.protection@emag.ro), the 11th of July 2020 (sent through the contact form from the website), of 18th of July 2020 (sent to info@emag.hu, data.protection@emag.ro, data.protection@emag.hu), after the start of the investigation by the Hungarian DPA, it erased the account of the claimant on 04.02.2021. The claimant was informed by Dante at the same date, by e-mail.

From the analysis of the proofs sent by the claimant, however it results that on 16th of July 2020 (probably, in the case of the request addressed through the contact form), [REDACTED] received an answer (from info@emag.hu, [REDACTED]) through which it is brought to his knowledge that the error message was forwarded to the competent colleagues. In this case, there was the possibility (as retained also above in the case of [REDACTED]) for the request for erasure of the data addressed by the claimant to be redirected without unjustified delays, to the internal addresses from the group dedicated to the handling of the requests based on the GDPR provisions.

Also, within the investigation, the controller brought to the knowledge of ANSPDCP that it has subsequently adopted as remediation measure the information of the teams for the

communication with the data subjects that they have the obligation to redirect internally the requests of the clients that report technical issues such as the rejection of some messages sent via e-mail.

We mention that Article 17 paragraph (1) letter b) of the GDPR provides the following:

"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(...)

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing."

The situation found in the case of [REDACTED] which, in contrast to [REDACTED], had addressed to the e-mail address dedicated to the submission of the requests based on GDPR (data.protection@emag.hu/emag.ro), proves that the establishment of a single and exclusive channel of communication that the data subjects can use, as well as the lack of an adequate information regarding some limitations from the technical point of view (such as the "e-mail filtering" solutions applied on the Dante servers) can lead to the groundless restriction of their rights.

Therefore, in this case a breach of the provisions of Article 12 paragraph (2) and of Article 17 paragraph (1) of the GDPR regarding the obligation of the controller to facilitate the exercise of the data subjects' rights and to delete personal data without undue delay is found.

Following the investigation, the controller amended its personal data policy published on the *emag* websites, by offering to the data subjects the possibility to send the requests based on the GDPR both by e-mail (at an address type data.protection@emag.hu) and by post/courier at a physical address from that country.

C. [REDACTED] Case

- IMI 311285 (Art. 61)

Object of the complaint

From the analysis of the documents sent, it is found that [REDACTED] claims that Dante has not communicated him what personal data it processes, following his request for change of the e-mail address associated to the *emag* account from 29th of March 2020. The claimant argues that, although he sent by post this request to Extreme Digital-eMAG Ltd. (received on 22nd of January 2021, by presenting the proof of delivery by post of this letter), he did not receive any answer. The request was sent to the address 1074 Budapest, Rákóczi út 70-72, mentioned on the website emag.hu, section dedicated to the processing of personal data, at the contact information of the controller Extreme Digital-eMAG Kft. In this request, the claimant was reporting also other aspects regarding the use of a voucher, for which he received an answer. The claimant did not present the actual copy of the request through which he claims that he exercised his right of access.

Moreover, the claimant shows that the e-mail address [REDACTED] was still processed by Dante (responses/messages received on this address on 26.11.2020, 28.12.2020, 25.01.2021 and on 28.01.2021), although he has requested its replacement with the address [REDACTED]; on 14.01.2021 he had requested on the e-mail information regarding the processing of his personal data, request that did not receive a request.

Conclusions:

From the investigation performed by ANSPDCP, no definite evidence regarding the fact that [REDACTED] exercised his right of access provided under Article 15 of the GDPR, through a letter sent to Extreme Digital-eMAG Korlátolt Felelősségű Társaság on 22.01.2021 could be retained. The controller sustained that no such request was received.

Regarding the request of rectification of the e-mail address of the claimant, from [REDACTED] to [REDACTED], although its initial request from 16.04.2020 was favourably solved on 15.05.2020, when the controller confirmed to the claimant the rectification of his e-mail address, the address [REDACTED] continued to be processed by Dante, in the context of a correspondence held with the claimant within the period November 2020 – January

2021, regarding the request of a voucher associated to a previous order (from 22.11.2019) correspondence that used this address. Thus, although the claimant has started the correspondence on 22.11.2020 from the address [REDACTED], the controller responded on the address [REDACTED], corresponding to the data from the order that was subject to the claim of the claimant. According to the statements of the controller, the e-mail address [REDACTED] continued to be saved in the database for the purpose of fulfilling the legal obligation to keep the accounting justifying documents, considering the electronic invoices previously provided.

We consider that this purpose of the processing is different from the one related to the handling of the claims, to the reactivation of this address and its use within the electronic correspondence would have been possible only based on the consent of the data subject, more as the context in which the claimant justified the request for rectification of the address based on the reason that it will be changed. Therefore, continuing to process the e-mail address [REDACTED], within the correspondence started on 22nd of November 2020, without the consent of [REDACTED] breaches the provisions of Article 6 paragraph (1) letter a) of the GDPR.

Within the investigation, the controller amended its internal procedure in order not to allow the use within the electronic correspondence with the data subject of an e-mail address for which a request for rectification previously existed.

II. Cooperation steps with the concerned supervisory authorities

Following the investigation performed, ANSPDCP electronically informed through IMI the other supervisory authorities, including the Hungary authority, within an informal consultation procedure, based on Article 60 from GDPR, regarding the conclusions resulted from the investigations performed within the three cases, as well as the intention of our institution to finalise them through a decision through which two fines and two corrective measures are to be applied, by detailing them (registration no. 440085). The only comment introduced by another supervisory authority was the one from the authority from France that does not consider to be a concerned authority.

As a result, a draft decision was drafted, based on the report and the minutes of findings drafted pursuant to Article 60 of Regulation (EU) 679/2016 and of Article 16 paragraph (3), (5), (6), (7) of Law no. 102/2005, republished (registered under no. 467153).

The Data Supervisory Authority from Hungary formulated in IMI, on 09.01.2023, both relevant and reasoned objections (with the proposal to establish the violation including of the provisions of Article 17 paragraph (1) of the GDPR in the case of the complaints submitted by [REDACTED] and [REDACTED] and of Article 13 paragraph (1) and Article 14 paragraph (1) of the GDPR, as well as with objections regarding the effectiveness, proportionality and dissuasiveness of the fines, proposing the application of a more severe fine), as well as comments (regarding the pre-checking of the newsletter section and the mandatory creation of an online account).

By considering the objections thus formulated, in accordance with Article 60 paragraph (4) of the GDPR, ANSPDCP reviewed the draft decision (registration no. 484845 from IMI), to which the concerned supervisory authorities did not submit any relevant and reasoned objections.

Following the receipt of some comments drafted by the Authority for the Personal Data Protection from Hungary on 21.02.2012, the draft of the decision was completed, thus resulting this final decision.

III. The minutes of the findings

Following the investigation carried out and the consultations with the other supervisory authorities, the minutes of the findings no. 7538/19.04.2023, through which the following deed were found, was drafted:

1. "At the date of this minutes, it is found that Dante International SA, with the identification data and headquarters mentioned on the first page of this minutes

has breached the provisions of Article 12 paragraph (2), in conjunction with Article 17 of the GDPR, as well as of Article 17 paragraph (1) of the GDPR regarding the controller's obligation to facilitate the exercise of data subjects and to delete personal data without undue delay, in particular in the case of the complaints submitted by [REDACTED] (for the request for the erasure of the data from 30.06.2020) and [REDACTED] (for the requests for the data erasure, submitted in July 2020), according to the findings from this minutes.

This deed represents the contravention provided under Article 12 of Law no. 190/2018, by reference to the provisions mentioned under Article 83 paragraph (5) letter b) of the GDPR.

2. At the date of this minutes, it is found that Dante International SA, with the identification data and headquarters mentioned on the first page of these minutes, violated the provisions of Article 13 paragraph (1) letters c), e), f) and Article 14 paragraph (1) letters c), e), f) of the GDPR, since at the start of the investigation (the date of the ANSPDCP's letter no. 21958 of 09.12.2021 sent to Dante International SA), the information on the emag.hu website did not contain complete information on the transfers to third countries, the purposes and recipients of the data in this context, according to the findings in this report

This deed represents the contravention provided under Article 12 of Law no. 190/2018, by reference to the provisions mentioned under Article 83 paragraph (5) letter b) of the GDPR.

3. At the date of this minutes, it is found that Dante International SA, with the identification data and headquarters mentioned on the first page of this minutes, has breached the provisions of Article 6 paragraph (1) letter a) of the GDPR, given that it continued to process the e-mail address [REDACTED] within the correspondence started on 22nd of November 2020, without the consent of the data subject, for the complaint submitted by [REDACTED], according to the findings from this minutes.

This deed represents the contravention provided under Article 12 of Law no. 190/2018, by reference to the provisions mentioned under Article 83 paragraph (5) letter a) of the GDPR."

Given that in this case Dante International SA performs a cross-border processing, the provisions of Article 60 of Regulation (EU) 2016/679 become applicable, as well as those of Article 16 paragraphs (3), (5), (6), (7) of Law no. 102/2005, republished, that provide for the application of the sanctions/corrective measures through a decision of the ANSPDCP's President, based on the minutes of control and findings drafted by the control personnel.

IV. Arguments and decision:

Considering the conclusions resulting from the investigations carried out at Dante International SA, a company that through the *emag* website (with versions in the official language of the three countries: Romania, Hungary and Bulgaria) carries out personal data processing operations in the context of ordering products which are sold online (directly or through partners), and the entities for which Dante International SA declares to be a data controller with its main headquarters are: DANTE INTERNATIONAL S.A., with its registered office in Romania, Extreme Digital-eMAG Korlátolt Felelösségi Társaság, with registered office in Hungary and EMAG INTERNATIONAL OOD, with registered office in Bulgaria,

Taking into account the relevant and reasoned objections sent by the Hungarian Data Protection Authority,

Having regard that, according to the latest records available from the National Trade Register Office (on 25.01.2023), the net turnover of DANTE INTERNATIONAL SA in 2021 was 7346114540 lei, for 2022 this information not being available yet,

Given that, from the verification of the ANSPDCP registers, it resulted that based on the GDPR there have been taken sanctions against Dante International SA, the only fines being of 3,000 EUR (Lei 14,420.4) for the processing without consent of the e-mail address of a claimant (the findings/sanction minutes no. 4471/27.02.2020), respectively of 1000 EUR (4918.6 lei) for non-compliance with the right to delete the data of a data subject (minutes of findings no. 21141/08.12.2022),

Based on the deeds found through the minutes of findings no. 7538/19.04.2023 above mentioned,

Considering the provisions of Article 12 paragraph (3) of the GDPR, according to which: "The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.", provisions applicable also for the exercise of the right to erasure of the data regulated under Article 17 of GDPR, as well as under Article 17 paragraph (1) of the GDPR regulating the obligation of the controller to delete personal data without undue delay, provisions which were breached for the complaints submitted by [REDACTED] and [REDACTED],

Since at the start of the investigation (date of ANSPDCP's letter no. 21958 of 09.12.2021, sent to Dante International SA), the information on the emag.hu website did not contain complete information on transfers to third countries, purposes and recipients in this context, according to the provisions of Article 13 paragraph (1) letters c), e), f) and Article 14 paragraph (1) letters c), e), f) of the GDPR,

By reference to the provisions of Article 6 paragraph (1) letter a) from GDPR, according to which the processing is legal only if and to the extent that the "data subject gave his/her consent for the processing of his/her personal data for one or more specific purposes", provision breached also in relation to the processing of the e-mail address of [REDACTED], which rectification was later on confirmed,

Considering that the fine that can be imposed for the violation of the provisions listed above is up to 20,000,000 EUR or, in the case of an undertaking, up to 4% of the total annual worldwide turnover corresponding to the previous financial year, according to Article 83 paragraph (5) letter b) and a) of the GDPR,

Having regard to the provisions of Article 83 paragraphs (1) – (3) of the GDPR, according to which:

"(1) Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

(2) Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- (b) the intentional or negligent character of the infringement;
- (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

(3) If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

Taking into account the criteria for individualising the fines established by Article 83 paragraph (2) and (3) of the GDPR, according to which the fines below were determined based, in particular, on the following aspects:

- the nature, gravity and duration of the infringement – non-compliance with the transparency conditions provided by Article 12 of the GDPR regarding the facilitation of the exercise of the rights of data subjects at the level of the company in Hungary (part of the Dante group) and implicitly, the non-immediate adoption of measures to delete personal data in the case of two data subjects from this country, according to Article 17 of the GDPR; failure to provide complete information on the emag.hu website in relation to the transfer of data to third countries, according to Article 13 and 14 of the GDPR; the policy for managing the requests of data subjects to exercise the rights provided for by the GDPR, which, at least in the case of the Hungarian company, limited the ways of submitting requests to a single communication channel (a dedicated email address);
- the negligent character of the controller's guilt in these cases;
- the mitigation measures of some of the reported issues, adopted by the controller during the investigations undertaken by the Hungary DPA and by the ANSPDCP, both in the particular cases of the petitioners, as well as regarding the general procedures applied by the controller;
- the types of personal data processed in the case of applicants – specific personal data for taking an online order, payment and delivery of the ordered product (in particular, name, surname, e-mail address, telephone number, delivery and/or billing address);
- the previous sanctions imposed by ANSPDCP against Dante International SA, a greater relevance presenting the fines mentioned above;

Taking into account the mitigating nature of some of the circumstances, such as: the small number of reported cases for which violations of the provisions of the RGPD were retained; failure to prove any damages suffered by the persons concerned/petitioners; adopting remedial measures for some of the reported issues; cooperation with the supervisory authority during the investigations undertaken; the relatively small number of sanctions consisting of fines applied previously,

Taking into account, in conclusion, the violations found, the elements of individualisation of sanctions, identified under Article 83 paragraph (2) of the GDPR, as well as the turnover of Dante International SA, based on which the ANSPDCP proceeded to analyse the effectiveness, proportionality and dissuasive effect of the fines applied,

The need to implement a method of anonymisation through which the risk of re-identification of the personal whose personal data are subject to this procedure to be prevented,

The importance of the regular training of the personnel from all the companies which are part of the Dante companies' group, in relation to the procedure that needs to be followed for the correct handling of the requests submitted by the data subjects based on the GDPR,

The groundless character of some of the aspects invoked within the complaints submitted by [REDACTED] and [REDACTED], according to the findings resulted from the investigations performed by ANSPDCP, above detailed, in relation to the procedure for the automatic creation of an account at the placement of an order on the *emag* websites and the pre-checking of the box regarding the receipt of newsletters (in the case of the complaint of [REDACTED]), respectively in relation to the exercise of the right to access (for the complaint of [REDACTED]), for which the procedure is to be followed according to Article 60 paragraph (9) of the GDPR,

Based on the provisions of Articles 14, 15 and 16 of Law no. 102/2005, republished, of Article 12 of Law no. 190/2018, with reference to Article 83 paragraphs (2) and (3) and to the provisions listed under Article 83 paragraph (5) letters a) and b) of Regulation (EU) 2016/679, in conjunction with the provisions of Article 58 paragraph (2) letters i) and d), as well as those of Article 60 of Regulation (EU) 2016/679, with reference to the provisions of Articles 24, 25 and 26 from the Procedure for conducting investigations, approved through the Decision of the ANSPDCP's President no. 161/2018, as well as on the provision of Government Ordinance no. 2/2001,

The National Supervisory Authority for Personal Data Processing

DECIDES

the following measures against Dante International SA:

1. The application of a fine in amount of Lei 148,830, the equivalent of 30,000 EUR, for the first deed found based on the minutes of findings no. 7538/19.04.2023, based on Article 83 paragraph (5) letter b) of Regulation (EU) 2016/679, for the breach of the provisions of Article 12 paragraph (2) and of Article 17 paragraph (1) of Regulation (EU) 2016/679;
2. The application of a reprimand for the second deed found based on the minutes of the findings no. 7538/19.04.2023, based on Article 58 paragraph (2) letter b) of Regulation (EU) 2016/679 for the breach of the provisions of Article 13 paragraph (1) letters c), e), f) and of Article 14 paragraph (1) letters c), e), f) of Regulation (EU) 2016/679;
3. The application of a fine in amount of Lei 49,610, the equivalent of 10,000 EUR, for the third deed found based on the minutes of findings no. 7538/19.04.2023 based on Article 83 paragraph (5) letter a) of Regulation (EU) 2016/679, for the breach of the provisions of Article 6 paragraph (1) letter a) of Regulation (EU) 2016/679;
4. Application of the corrective measure provided by Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 to ensure the full information of data subjects, by providing all the information mentioned in Articles 13 and 14 of Regulation (EU) 2016/679, including in the context of the transfer of personal data to third countries, information to be available on *emag* websites managed by the controller, in the national language version of each country – deadline: 30 days from on the date of communication of this decision;
5. The application of the corrective measure provided under Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 to implement an anonymisation method in order to prevent the risk of re-identification of the persons whose personal data are subject of this procedure, according to Article 32 of Regulation (EU) 2016/679 – deadline: 30 days as of the communication of this decision;
6. The application of the corrective measure provided under Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 to take measures for the regular training of the personnel from the companies from Romania, Hungary and Bulgaria, that are part of the Dante companies' group, in relation to the procedure that needs to be followed for the correct handling of the requests submitted by the data subjects based on Regulation (EU) 2016/679 – deadline: 30 days as of the communication of this decision.

Dante International SA will communicate to ANSPDCP the measures taken for the application of the corrective measures within 45 days as of the receipt of this decision.

This decision was subject to the procedure provided under Chapter VII of Regulation (EU) 2016/679, being provided to the concerned supervisory authorities.

According to Article 15 paragraph (6) of Law no. 102/2005, republished, when applying the fine, the official exchange rate of the National Bank of Romania of 17.05.2023, hour 14:28 was taken into consideration (EUR 1= Lei 4.9610).

According to the provisions of Article 17 paragraph (3) from Law no. 102/2005, republished, **Dante International SA** has the obligation to pay the fine within 15 days as of the communication of the minutes of the findings (attached in copy) and of this decision, contrary following to be proceeded to enforcement.

The fine will be paid in the account of the State Treasury where **Dante International SA** has his fiscal headquarters, account code 20A350102, within 15 days from communication, following for a copy of the receipt or payment order to be sent to the National Supervisory Authority for Personal Data Processing within the same deadline.

Article 83 of Regulation (EU) 679/2016 only provides for the maximum threshold of the fines that can be applied, not for their minimum limit, so that Article 28 paragraph (1) of Government Ordinance no. 2/2001, with its subsequent amendments and completion, regarding the possibility to pay half of the minimum of the fine provided under the normative act, does not apply in this case.

This decision, together with the minutes no. 7538/19.04.2023 (attached in copy), is communicated to **Dante International SA** that it has the right to challenge them, according to Article 17 of Law no. 102/2005:

"Article 17

- (1) The data controller or processor may file an appeal against the report of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be, with the administrative contentious section of the competent court, within 15 days from handing, respectively from communication. The decision resolving the appeal can be appealed only by appeal. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania.
- (2) The report of finding/sanctioning or the decision of the president of the National Supervisory Authority unchallenged within 15 days from the date of handing, respectively the communication, constitutes an enforceable title without any other formality. Introducing the appeal provided in paragraph (1) suspends only the payment of the fine, until a final court decision is issued.
- (3) The deadline of payment of the fine is 15 days from the date of handing, respectively from the date of communication of the minutes of finding/sanctioning or of the decision of the president of the National Supervisory Authority."

President,



CONTROL DEPARTMENT

No. _____ / _____

Decision

following the investigation performed at la SC UiPath SRL

The National Supervisory Authority for Personal Data Protection, with the headquarters in 28-30 G-ral Gheorghe Magheru Blvd., District 1, post code 010336, Bucharest, legally represented by [REDACTED], President, issues this decision against SC UiPath SRL, with the headquarters in 4 and 11, Vasile Alecsandri and Constantin Daniel Street, Building A, 5th – 6th Floor, District 1, Bucharest, registered with the Trade Registry under no. J40/8216/2015, sole registration code 34737997, legally represented by [REDACTED], as director

Considering the following:

I. Personal data security breach notification received based on Article 33

SC UiPath SRL notified a personal data security breach, by filling in the form regarding the breach of the personal data security provided under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), notification registered at the National Supervisory Authority for Personal Data Processing under no. 23973/07.12.2020 (by e-mail) and no. 2699/12.02.2021 (on-line).

Considering that the main establishment of the controller that performs activities in several Member States is the one from Romania, ANSPDCP is the supervisory authority of the main establishment of the controller, competent to act as lead supervisory authority for the cross-border processing performed by UiPath SRL according to the procedure provided under Article 60 of the GDPR, being at the same time the only supervisory authority from the EU to which the personal data security breach was notified.

Therefore, the National Supervisory Authority for Personal Data Processing (hereinafter referred to as „ANSPDCP”) introduced within the application “Internal Market Information System” a notification according to Article 56 registered under no. 294927.1, in order to inform the supervisory authorities from the other European Union Member States.

Therefore, according to the mentions from the notification forms no. 23973/07.12.2020 (by e-mail) and no. 2699/12.02.2021 (on-line), on 1st of December 2020, 20:41 time, a breach of the personal data confidentiality estimated to have taken place on 30th of November 2020 was identified, consisting of the publishing of the personal data (user's first name and last name associated to the Academy Platform Account, user name, unique identifier of each user, e-mail address, name of the company where the user is employed, country and details on the level of knowledge level obtained within the UiPath Academy courses) of 600,000 users of the Academy

Notă Informare RGPD

https://www.dataprotection.ro/?page=Informare_protecția_datelor_conf_GDPR

Platform on the website accessible at the URL address www.raidforums.com, information brought to the knowledge of the controller by a third party.

The „Academy Platform” was made available to the users in order to get familiar with the products marketed by UiPath, the latter being rewarded with a certification of the knowledge obtained. The access of the users to the Platform is performed through an account, all the data (above) being stored in a common database.

Based on the technical analysis performed by the controller, the latter found that the **technical settings of the storage space allowed the unauthorized access** to the personal data of the Academy Platform users. (At this moment the access is performed through a multi-factor authentication system single-on type, being limited to the persons entitled, based on some unique identification elements and on a password with complex elements).

The technical and organisational measures applied by the controller consisted of the prevention of the unauthorised and unauthenticated access, of the blocking of the unauthorised accessing source, a formal notification being submitted with the administrator of the third-party website with the request to eliminate that file.

The controller considered that the incident **is not likely to generate a high risk** for the data subjects (users of the Academy Platform), their information not being necessary, without excluding that, following the final analysis, the decision on their information to be taken, according to the notification submitted.

II. Conclusions following the investigation performed at SC UiPath SRL:

From the investigation performed by ANSPDCP, the following resulted:

- the security incident consisted of the publishing of the personal data of the Academy Platform users on 30th of November 2020 at the URL address www.fileconvoy.com, where there have been redirected through a link accessible at the URL address www.raidforums.com; the data of the Academy Platform users were exposed during 30th of November 2020 – 9th of December 2020, persons from several EU Member States being affected;
- at this moment, “a very small part of the data continues to be found on www.raidforums.com, in the form of a preview”;
- the personal data affected by the incident: user's first name and last name associated to the account from the Academy Platform, the e-mail address, unique identifier of each user, the name of the company where the user is employed, the country and details on the level of knowledge obtained within the UiPath Academy courses;
- from the investigation it resulted that no special categories of personal data were affected;
- SC UiPath SRL implemented, before the incident notified, a security management system (ISMS) according to the ISO/IEC 27001:2013 standard, which is annually audited; according to the conclusions of the audit report from 20th of March 2020, phase 2, it was found as early as 2019 in phase I that there is an improvement possibility in relation to the risks' evaluation; in phase 2, given that no activity in relation to this improvement possibility was performed, this remains open;
- before the incident took place, the controller implemented cybersecurity and confidentiality policies (on: the correct use of the technology, the access control, the work on own devices, cryptographic control, data retention, transfer and erasure, incidents' management, information classification, management of devices, network and

communications security, passwords, physical protection, security of the information disclosed by providers, teleworking, confidentiality, authorised external audit, as well as the plan for the continuance of the business (security), procedure on the storage of the documents and code of conduct);

- the annually reviewed policies are brought to the knowledge of the employees both at the hiring and periodically, during the employment;
- the employees receive warnings in relation to the need of performing the training, and each team leader receives reports in relation to the stage in which his team is in relation to the annual training; the policies are reviewed annually and are brought to the knowledge of the employees both annually and periodically;
- after the incident, the controller took the following measures:
 - established a plan for the reinforcement of the security of the storage accounts in cloud; the public storage accounts will be annually reviewed by the internal security team. Within the review procedures the details regarding the data stored in each such account will be recorded, as well as the reason for which that storage accounts are public;
 - added new policies within the storage platform of these accounts (Microsoft Azure) in order to ensure that all the storage accounts are implicitly created **privately**;
 - shall implement penetration tests in order to evaluate the security of the systems;
- SC UiPath SRL performed the information of the data subjects both by e-mail and through the UiPath Academy Platform;
- following the introduction of the case within the IMI application, the following Member States declared themselves as concerned supervisory authorities: Germany – Lower Saxony Land, Italy, Ireland, Slovenia, Belgium, Norway, Estonia, Austria, Netherlands, Finland, Sweden, Luxembourg, Spain, Bulgaria, Germany – Hessen Land, France and Denmark;
- following the investigation steps taken it was found that a number of 600,000 data subjects were affected, from 258 states, out of which 76,095 data subjects from the EU/EEA Member States;
- from the reviews performed until the date of conclusion of the report, it was found that no complaints were submitted by the persons concerned by the security incident notified by SC UiPath SRL.

III. Information of the concerned supervisory authorities within IMI

On 17th of May 2021, the other supervisory authorities were informed through the IMI application, registered under no. 294927.1, within a LSA and CSA identification procedure (based on Article 56 of the GDPR), in relation to the security incident, as well as in relation to the intention of our authority to act as lead supervisory authority, with deadline until 07.08.2021.

Until the date of this report, the following supervisory authorities declared as concerned supervisory authorities – CSA:

- the Supervisory Authority from Germany – Lower Saxony Land (with the mention "the data subjects from Lower Saxony could be affected");

- the supervisory authorities from Italy, Ireland, Slovenia, Belgium, Norway, Estonia, Austria, Netherlands, Finland, Sweden, Luxembourg, Spain, Bulgaria, Germany – Hessen land, France, Denmark (with the mention “the processing is affecting or could substantially affect the data subjects from those states”);
- the supervisory authority from Germany – Baden-Wurttemberg Land did not declare itself as concerned authority.

The concerned supervisory authorities did not submit relevant and reasoned objections, thus resulting this final decision.

IV. The findings/sanctioning report

Following the investigation performed, the findings/sanctioning report no. 13172 through which the following aspects were found was concluded:

*“On the conclusion date of this report, 10.07.2023, it was found that SC UiPath SRL, with the identification data and headquarters mentioned on the first page of this report, breached the provisions of Article 25 paragraph (2) and Article 32 paragraph (1) letters b) and d) and paragraph (2) of the GDPR, as it did not implement adequate technical and organisational measures in order to ensure that, implicitly, the personal data cannot be accessed, without a person’s intervention, by an unlimited number of data subjects, including the capacity to ensure the continued confidentiality and resistance of the processing systems and services, as well as a process for the periodical testing, evaluation and of the efficiency of the technical and organisational measures in order to guarantee the security of the processing. This led to the **unauthorised disclosure and unauthorised access** to the personal data (first name and last name of the user associated to the Academy Platform account, user name, unique identifier of each user, the e-mail address, the name of the company where the user is employed, the country and details on the level of knowledge obtained within the UiPath Academy courses) of approximately 600,000 users of the Academy Platform belonging to the controller UiPath (out of which 76,095 data subjects from the EU/European Economic Area), during 30th of November 2020 – 9th of December 2020, at the URL address www.fileconvoy.com (where they have been redirected through a link accessible at the URL address www.raidforums.com), fact that can lead specifically to physical, material or moral damages for the natural persons affected, such as the loss of the control on their personal data or the loss of the personal data confidentiality through professional secret or another economic or social significant disadvantage for that natural person.*

This deed represents a contravention according to Article 12 of Law no. 190/2018, by reference to the provisions mentioned under Article 83 paragraph (4) letter a) of Regulation (EU) 2016/679.”

Considering the findings from the investigation performed at SC UiPath SRL, as well as from the analysis of the incident according to the criteria from Article 83 of the GDPR, the provisions of Article 60 of Regulation (EU) 679/2016, as well as those of Article 16 paragraphs (3) and (7) of Law no. 102/2005, republished, that provide for the application of sanctions/corrective measures through the decision of the President of ANSPDCP, based on the findings report and of the report of the control personnel, become applicable.

V. Arguments and resolution:

Considering the conclusions resulting from the investigation performed at SC Uipath SRL,

Based on the deed found through the findings report no. 13172/10.07.2023, above mentioned,

Considering the provisions of Article 25 paragraph (1) and (2) of the GDPR, according to which: "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

Considering the provisions of Article 32 paragraph (1) letter b) and paragraph (2) of the GDPR, according to which "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"

Considering that the fine that can be applied for the breach of the controller's obligations mentioned above is of up to EUR 10,000,000 or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, according to Article 83 paragraph (4) letter a) of the GDPR,

Considering the provisions of Article 83 paragraphs (1), (2) and (3) of the GDPR,

"(1) Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

(2) Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them
- b) the intentional or negligent character of the infringement
- c) any action taken by the controller or processor to mitigate the damage suffered by data subjects
- d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

- e) any relevant previous infringements by the controller or processor;
- f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- g) the categories of personal data affected by the infringement;
- h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

(3) If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

Considering the fine individualisation criteria established under Article 83 paragraphs (2) and (3) of the GDPR, depending on which the below fine was established based, mainly, on the following aspects:

- a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them:
 - 600,000 data subjects affected (users of the Academy Platform);
 - the technical settings of the storage space that allowed the unauthorized access to the personal data of the Academy Platform users;
 - the incident that took place on 30th of November 2020 consisted of the publishing of the personal data on a third-party website, information brought to the knowledge of the user by a third party;
 - no complaints were submitted by the data subjects concerned by the security incident notified by SC Uipath SRL, therefore no damages suffered by them were able to be identified;
- b) the intentional or negligent character of the infringement
 - out of negligence;
- c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
 - the data subjects concerned by the incident were subsequently notified, by e-mail and through the Uipath Academy platform;
 - after the security incident took place additional technical and organisational measures were adopted;
- d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
 - the controller implemented cybersecurity and confidentiality policies;
- e) any relevant previous infringements by the controller or processor;
 - no previous breaches were identified;
- f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement:

- the controller notified the security incident within the deadline provided under GDPR and submitted to ANSPDCP all the information requested within the investigation performed;
- g) the categories of personal data affected by the infringement:
- first name and last name user associated to the Academy Platform Account, user name, unique identifier of each user, e-mail address, name of the company where the user is employed, country and details on the level of knowledge level obtained within the UiPath Academy courses. No special categories of personal data have been affected.
- h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement:
- the controller notified the security incident within the deadline provided under GDPR and submitted to ANSPDCP all the information requested within the investigation performed;
- i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures:
- no measures were applied previously;
- k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement:
- we considered that the security incident took place out of negligence, and not for avoiding some losses or obtaining some financial benefits directly or indirectly.

Considering, in conclusion, the breaches found, the elements for the individualization of the sanctions, identified based on Article 83 paragraph (2) and paragraph (3) from the GDPR, based on which ANSPDCP proceeded to the analysis of the effectiveness, proportionality and dissuasive effect of the fines applied,

Based on Articles 14, 15 and 16 of Law no. 102/2005, republished, of Article 12 of Law no. 190/2018, by reference to Article 83 paragraph (2) and to the provisions detailed under Article 83 paragraph (4) letter a) of Regulation (EU) 2016/679, corroborated with the provisions of Article 58 paragraph (2) letter i), as well as those of Article 60 from Regulation (EU) 2016/679, by reference to the provisions of Article 24 and 26 of the Procedure for conducting investigations, approved by Decision of the President of ANSPDCP no. 161/2018, with the subsequent amendments and completions, we propose the following:

**The National Supervisory Authority for Personal Data Processing
DECIDES**

The following measures against SC UiPath SRL:

- to impose a fine in amount of Lei 346,598, the equivalent of EUR 70,000, for the deed found based on the findings report no. 13172 from 10.07.2023 based on Article 58 paragraph (2) letter i) and Article 83 paragraph (4) letter a) of Regulation (EU) 679/2016, for the breach of Article 25 paragraphs (1) and (2) and Article 32 paragraph (1) letter b) and paragraph (2) of the GDPR;
- to apply the corrective measures provided under Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 consisting of the implementation of a procedural mechanism and applied at regular time intervals, regarding the testing, evaluation and periodical evaluation of the efficiency of the measures taken, considering the risk

GDPR Information Form

<https://www.dataprotection.ro/?page=Informare protectia datelor conf GDPR>

represented by the processing, in order to ensure a corresponding level of security and to avoid in the future similar security incidents – deadline: 30 days as of the communication of this decision.

This decision is subject to the procedure provided under Chapter VII of Regulation (EU) 2016/679, being provided to the concerned supervisory authorities.

According to Article 15 paragraph (6) of Law no. 102/2005, republished, when applying the fine, the official exchange rate of the National Bank of Romania of the 10th of July 2023, hour 15 was taken into consideration (EUR 1= Lei 4.9514).

According to the provisions of Article 17 paragraph (3) of Law no. 102/2005, republished, **SC UiPath SRL** has the obligation that within 15 days as of the communication of the report of findings (attached in copy) and of this decision to pay the fine, contrary following to be proceeded to enforcement.

The fine will be paid in the account of the State Treasury where **SC UiPath SRL** has his fiscal headquarters, account code 20A350102, within 15 days from communication, following for a copy of the receipt or payment order to be sent to the National Supervisory Authority for Personal Data Processing within the same deadline.

Article 83 from Regulation (EU) 679/2016 only provides for the maximum threshold of the fines that can be applied, not for their minimum limit, so that Article 28 paragraph (1) from GO no. 2/2001, with its subsequent amendments and completion, regarding the possibility to pay half of the minimum of the fine provided under the normative act, does not apply in this case.

This decision, together with the report of findings no. 13172 of 10.07.2023 (attached in copy), is communicated to **SC UiPath SRL** that has the right to challenge them, according to Article 17 from Law no. 102/2005:

"Article 17

- (1) The data controller or processor may file an appeal against the report of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be, with the administrative contentious section of the competent court, within 15 days from handing, respectively from communication. The decision resolving the appeal can be appealed only by appeal. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania.
- (2) The report of finding/sanctioning or the decision of the president of the National Supervisory Authority unchallenged within 15 days from the date of handing, respectively the communication, constitutes an enforceable title without any other formality. Introducing the appeal provided in paragraph (1) suspends only the payment of the fine, until a final court decision is issued.
- (3) The deadline of payment of the fine is 15 days from the date of handing, respectively from the date of communication of the minutes of finding/sanctioning or of the decision of the president of the National Supervisory Authority.

President,



Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2023-08-24, no. DI-2021-10388. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-10388
IMI case no. 164557

Date of decision:
2023-08-24

Date of translation:
2023-08-25

Decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Klarna Bank AB has now complied with the complainant's request for deletion. Against this background, the Swedish Authority for Privacy Protection finds no reason to take further action in the case.

The case is closed.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision against Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY as responsible supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR).¹ The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In the light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Denmark, Finland, Italy, Poland and Austria.

Complaint

The complainant has mainly stated that Klarna continued to send him e-mails even though he requested erasure of his personal data.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

¹ Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

What Klarna has stated

In its opinion to IMY, Klarna Bank AB stated, *inter alia*, that the company will erase the complainant's personal data. In a second opinion, Klarna confirmed that the erasure of the complainant's personal data has been completed.

Statement of reasons for the decision

The complainant has requested the erasure of his personal data. The right to erasure derives from Article 17 of the GDPR. The provision implies that in certain cases, data subjects have the right to have their personal data erased without undue delay.

Klarna has stated that the company has now erased the complainant's data. IMY has no reason to question this. IMY concludes that Klarna has now complied with the complainant's request for deletion. Against this background, IMY finds no reason to take any further action in this case.

The case is closed.

This decision has been approved by the specially appointed decision-maker [REDACTED]
[REDACTED] after presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Swedish Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Swedish Authority for Privacy Protection if it does not contain any sensitive personal data or information that may be subject to confidentiality. The authority's contact information is shown on the first page of the decision.



Deliberation No 82/RECL28/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 2.888 lodged against the company [REDACTED] via IMI Article 56 procedure 61804

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Spain submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: [REDACTED]) via IMI in accordance with Article 56 procedure - 61804.
2. The complaint was lodged against the controller [REDACTED] ([REDACTED]), who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. Pursuant to the original IMI request, the complainant’s son, aged three year, received a promotional (paper) mail regarding [REDACTED], whilst the latter has never been in any commercial relation with the Controller.
4. The complaint thus concerns the origin and subsequently the objection to any further use of the personal data for marketing reasons.

5. In essence, the complainant asks the CNPD to check on the origin of the personal data of his son and requires his right to object.
6. The complaint is therefore based on Articles 15 and 21 of the GDPR.
7. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's son's data, and in particular with regard to the origin of the personal data with the controller and the right to erasure.
8. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

9. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
10. In accordance with Article 15 of the GDPR "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information (...) (g) where the personal data are not collected from the data subject, any available information as to their source*";
11. In accordance with Article 21 (2) of the GDPR, "*where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing*";
12. Article 56(1) GDPR provides that "*(...) the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing*

**Deliberation No 82/RECL28/2023 of 22 September 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 2.888 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 61804**

carried out by that controller or processor in accordance with the procedure provided in Article 60”;

13. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other*";
14. According to Article 60(3) GDPR, "*The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views*";

2. In the present case

15. Following the intervention of the CNPD, the Controller confirmed that:
 - a customer of the controller different from the complainant (someone close to the complainant's son), who was eligible for the promotional direct mail campaign, used the name, surname and address of the complainant's son as the delivery and billing address information on his account. Whilst the promotional mail was intended for this customer of the controller, the mail was sent to the complainant's son, which was not the intention of the controller.
 - the controller has ensured that no future promotional mailing and marketing will be sent to the name, surname and address of the complainant's son.
 - the controller responded to the complainant to inform him that the controller has taken the above actions.
 - as an additional information, the controller only directs its promotional communications to existing customers (who have registered active accounts with the controller) who have not exercised their choice to opt out of receiving direct mail marketing. (Customers in Spain can change this preference at any time, via [REDACTED]; which is also explained in the controller's Privacy Notice, under the heading “*What Choices Do I Have?*”) In this sense, the controller uses eligible customers' last used billing address as the address to send the direct mail.



Deliberation No 82/RECL28/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 2.888 lodged against the company [REDACTED] via IMI Article 56 procedure 61804

3. Outcome of the case

16. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to provide the complainant the necessary information and honored the right to object, in accordance with Articles 15 and 21 of the GDPR.
17. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
18. The CNPD then consulted the supervisory authority of Spain, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Spain, has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 2.888 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 22 September 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner



**Deliberation No 82/RECL28/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 2.888 lodged against the company [REDACTED]
[REDACTED] via IMI Article 56 procedure 61804**

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

**Deliberation No 83/RECL29/2023 of 22 September 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 3.633 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 73526**

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria, Germany, submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: [REDACTED]) via IMI in accordance with Article 61 procedure - 73526.
2. The complaint was lodged against the controller [REDACTED], who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

[REDACTED] did not act on the complainant’s request regarding the access to his personal data [REDACTED] is processing. Furthermore [REDACTED] addressed several e-mails to the complainant using the wrong name.
4. In essence, the complainant asks the CNPD to request [REDACTED] to grant him access to his personal data and to rectify this personal data.

5. The complaint is therefore based on Articles 15 and 16 of the GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right of access and rectification.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 15 of the GDPR "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information (...)*";
10. In accordance with Article 16 of the GDPR "*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her (...)*";
11. Article 56(1) GDPR provides that "*(...) the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60*";
12. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the*

Deliberation No 83/RECL29/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 3.633 lodged against the company [REDACTED] via IMI Article 61 procedure 73526

supervisory authorities concerned shall exchange all relevant information with each other";

13. According to Article 60(3) GDPR, "*The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views*";

2. In the present case

14. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
15. The controller's customer service team was in contact with the complainant regarding order related topics and that in the e-mail conversation the complainant asked for access to his personal data. The controller then replied to the complainant that he could submit the data subject access request via the designated contact form when logged in to the customer account, but the complainant did not utilise this option or otherwise contact the controller again regarding his request. As the data subject request was made outside the contact form, the controller required additional verification for the complainant in this case (as there are two accounts for that delivery address with nearly identical emails) and therefore contacted him again.
16. Regarding the request for data rectification, the controller reviewed its systems and confirmed that the name in the customer account connected to the e-mail address (AAA) is the name of the complainant and that no other name is registered in the controller's systems to that account or has been used in communications associated with that customer account.
17. The complainant ([REDACTED]) forwarded to the controller an email the controller sent to a different e-mail address, (BBB), which is linked to a separate ([REDACTED]) customer account ([REDACTED]); this second account is registered with the name of a different person (same family name) and includes the same delivery address as the complainant. In mails to the email address (BBB), the controller used the name ([REDACTED]) which is the registered name of the holder of that account in the controller's systems. By contrast, in e-mails to the customer account associated with the e-mail address (AAA), the controller used the name ([REDACTED]) which is the registered name of the holder of that account in the controller's systems. Therefore, the controller could not find any name data which the controller would



Deliberation No 83/RECL29/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 3.633 lodged against the company [REDACTED] via IMI Article 61 procedure 73526

have to rectify pursuant to Article 16 GDPR. In addition, as customers can change names associated with their account through a setting, the controller contacted the complainant to enable him to change his name in his account, if he wished to do so.

3. Outcome of the case

18. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller did not refuse to act on the complainant's right of access and rectification, in accordance with Articles 15 and 16 of the GDPR. With two nearly identical email addresses belonging to two persons having the same family name and delivery address, additional verification seemed necessary. Also it seemed obvious, based on the evidence, that the complainant [REDACTED] also had access to the other email account of [REDACTED]

19. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

20. The CNPD then consulted the supervisory authority of Bavaria, Germany, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria, Germany, has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 3.633 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 22 September 2023

The National Data Protection Commission



**Deliberation No 83/RECL29/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 3.633 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 73526**

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2023-09-28, no. IMY-2023-8429. Only the Swedish version of the decision is deemed authentic.

Diarienummer:
IMY-2023-8423

Datum:
2023-10-31

Decision under the General Data Protection Regulation – Resursforum Sverige AB

Decision of the Privacy Protection Authority

The Privacy Protection Authority (IMY) notes that, on 15 July 2022, Resursforum Sverige AB (556706-7607) has processed personal data in breach of Article 12(4) of the GDPR¹ by not informing the complainant of the reason why Resursforum Sverige AB rejected the complainant's request for rectification pursuant to Article 16 of the Data Protection Regulation and by not providing the complainant with information about its ability to lodge a complaint with the Responsible Supervisory Authority for judicial review of the refusal.

IMY gives Resursforum Sverige AB a reprimand pursuant to Article 58(2)(b) GDPR for breach of Article 12(4) GDPR.

Presentation of the supervisory case

IMY has initiated supervision against Resursforum Sverige AB in response to a complaint.

The complaint shows, in essence, the following: The complainant requested rectification of his personal data on 21 June 2022. On 15 July 2022, Resursforum Sverige AB rejected the complainant's request without justification. In connection with the refusal, Resursforum Sverige AB has not provided information to the complainant about the possibility of filing a complaint with the lead supervisory authority for judicial review of the refusal.

In its opinion on 27 June 2023, Resursforum Sverige AB stated the following. Resursforum Sverige AB has not informed the complainant of the reasons for the refusal and of the right to lodge a complaint with the lead supervisory authority for judicial review of the refusal. Resursforum Sverige AB has taken steps for new routines regarding the handling of similar cases and wrote a non-conformity report.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

The complaint has been submitted to IMY, as the lead supervisory authority under Article 56 GDPR, by the supervisory authority in Denmark where the complaint was lodged. In view of the cross-border complaint, IMY has made use of the cooperation

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

and consistency mechanisms provided for in Chapter VII of the GDPR. The supervisory authority concerned has been the data protection authority in Denmark.

Statement of reasons for the decision

Legal Regulation

If the controller fails to act upon the data subject's request, the controller shall without delay and no later than one month after they received the request to inform the data subject of the reasons for non-action and of the possibility of lodging a complaint with a supervisory authority and requesting judicial review under Article 12(4) GDPR.

The Privacy Protection Authority's assessment

Has there been a breach of the GDPR?

Resursforum Sverige AB states that it has not informed the complainant of the reasons for rejecting the complainant's request for rectification and of the possibility of lodging a complaint with the lead supervisory authority for judicial review of the refusal. IMY finds that Resursforum Sverige AB has thereby processed personal data in breach of Article 12(4) of the GDPR.

Choice of intervention

According to Article 58(2)(i) and Article 83(2) of the GDPR IMY has the power to impose administrative fines pursuant to Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. In addition, it is clear from Article 83(2) which factors must be taken into account when imposing administrative fines and in determining the amount of the fine. In the case of a minor infringement, the IMY may, as stated in recital 148, instead of imposing a pecuniary penalty, issue a reprimand under Article 58(2)(b). Account must be taken of aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous relevant infringements.

IMY notes the following relevant circumstances. The violations have occurred to a single data subject. Resursforum Sverige AB has stated that it has taken measures for new procedures for handling similar cases. Resursforum Sverige AB has not previously received any corrective action for breach of the General Data Protection Regulation. In those circumstances, IMY considers that there are such minor infringements within the meaning of recital 148 and that it is therefore appropriate to refrain from imposing a fine on Resursforum Sverige AB for the infringements found. IMY gives Resursforum Sverige AB a reprimand pursuant to Article 58(2)(b) GDPR for breach of Article 12(4) GDPR.

This decision was taken by Head of Unit [REDACTED] following a presentation by [REDACTED].

[REDACTED], 2023-10-31 (This is an electronic signature)

How to appeal

If you want to appeal the decision, write to the Privacy Protection Authority. Please indicate in the letter the decision you are appealing and the amendment you are requesting. The appeal must have been received by the Swedish Integrity Protection Authority no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Integrity Protection Authority will forward it to the Administrative Court in Stockholm.

You can e-mail the appeal to the Privacy Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact details are shown in the first page of the decision.

Notice: This document is an official translation of the Swedish Authority for Privacy Protection's decision on 2023-10-17, no. DI 2020 10545. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI 2020 10545, IMI case no.
66536

Date of decision:
2023 10 17

Final decision under the General Data Protection Regulation – H & M Hennes & Mauritz GBC AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that H&M Hennes & Mauritz GBC AB has processed personal data in breach of Article 12.3 and 21.3 of the General Data Protection Regulation (GDPR)¹ by

- regarding complaint 1: continuing to process personal data for direct marketing purposes after the complainant objected to such processing on 5 April 2019 in accordance with the right under Article 21(2),
- regarding complaint 2: continuing to process personal data for direct marketing purposes after the complainant objected to such processing on 4 July 2019 in accordance with the right under Article 21(2),
- regarding complaint 3: continuing to process personal data for direct marketing purposes after the complainant objected to such processing on 3 September 2019 in accordance with the right under Article 21(2),
- regarding complaint 4: continuing to process personal data for direct marketing purposes after the complainant objected to such processing on 31 July 2018 in accordance with the right under Article 21(2),
- regarding complaint 5: continuing to process personal data for direct marketing purposes after the complainant objected to such processing on 8 August 2019 in accordance with the right under Article 21(2),
- regarding complaint 6: continuing to process personal data for direct marketing purposes after the complainant objected to such processing on 8 August 2019 in accordance with the right under Article 21(2).

Postal address:
Box 8114
104 20 Stockholm

Website:
www.my.se

E-mail:
my@my.se

Phone:
08 657 61 00

¹ Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)

The Swedish Authority for Privacy Protection finds that H&M Hennes & Mauritz GBC AB has processed personal data in breach of Article 6.1 of the General Data Protection Regulation by

- regarding complaint 1: processing the complainant's personal data for direct marketing purposes between 7 April 2019 and 2 August 2019 without having a legal basis after the complainant objected to such processing,
- regarding complaint 2: processing the complainant's personal data for direct marketing purposes between 6 July 2019 and 3 October 2019 without having a legal basis after the complainant objected to such processing,
- regarding complaint 3: processing the complainant's personal data for direct marketing purposes between 5 September 2019 and 5 February 2020 without having a legal basis after the complainant objected to such processing,
- regarding complaint 4: processing the complainant's personal data for direct marketing purposes between 2 August 2018 and 16 February 2020 without having a legal basis after the complainant objected to such processing,
- regarding complaint 5: processing the complainant's personal data for direct marketing purposes between August 2018 and May 2019 without having a legal basis after the complainant objected to such processing,
- regarding complaint 6: processing the complainant's personal data for direct marketing purposes between 10 August 2019 and 15 September 2019 without having a legal basis after the complainant objected to such processing,

The Swedish Authority for Privacy Protection finds that H&M Hennes & Mauritz GBC AB, regarding aspects of complaints, has processed personal data in breach of Article 12(2) of the GDPR by not ensuring systems and procedures that have sufficient capacity to facilitate the complainants' exercise of the right to object to direct marketing.

On the basis of Articles 58(2) and 83 of the GDPR, the Swedish Authority for Privacy Protection decides that H&M Hennes & Mauritz GBC AB shall pay an administrative fine of SEK 350 000 (ca 31 000 €) for the infringements found.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding H&M Hennes & Mauritz GBC AB (H&M or the company) due to aspects of complaints. The complaints have been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the countries where the complainants have lodged the complaints (Portugal, Italy and The United Kingdom) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been hand ed through wr tten procedure. In the ght of the comp a nt re at ng to cross-border process ng, IMY has used the mechan sms for cooperat on and cons stency conta ned n Chapter VII of the GDPR. The superv sory author tes concerned have been the data protect on author tes n Germany, S oven a, France, Denmark, Spa n, Norway, Ita y, F n and, Po and, Be g um, Portuga , Cyprus, Eston a and Nether ands.

As comp a nts 4 and 5 have been subm tted by the Un ted K ngdom, wh ch has eft the Un on dur ng the per od of the superv sory procedure, IMY has been n contact w th the UK Superv sory Author ty (ICO) to ensure that a ne b s n dem s tuat on s avo ded. The ICO has no nformat on that t has taken any correct ve act on n regards to the comp a nts. It s noted that the ICO s retent on per od for comp a nts s two years and therefore they have not kept any nformat on on the comp a nts. Furthermore, IMY notes that the contro er n quest on, wh e commun cat ng w th IMY, has not nd cated that any such measures had been taken by the ICO. It s apparent from Art c e 3 of the GDPR that the prov s ons of that regu at on app y to a process ng of persona data carr ed out n the context of the act v tes of the contro ers estab shment w th n the Un on, whether or not the process ng was carr ed out w th n the Un on. IMY therefore cons ders that there s no mped ment to the nc us on of comp a nts 4 and 5 n IMY s superv s on.

What the complainants and Hennes & Mauritz GBC AB has stated in general

Accord ng to the comp a nts, the comp a nts rece ved unwanted news etters from the company even though they objected to hav ng the r persona data processed for d rect market ng purposes.

The company has stated that t s the data contro er for the process ng to wh ch the comp a nts re ate.

The company offers ts customers three d fferent ways to oppose market ng v a news etters. Customers can change the r subscr pt on status under the r account sett ngs, unsubscr be v a a nk prov ded n each news etter ma ng or contact the company s customer serv ce. The company hand es a very arge number of subscr bers annua y and on y n a very sma part of dereg strat on cases does some sort of prob em ar se.

The company conf rms that t has rece ved the comp a nants' object ons n a comp a nts. However, the company has no documented correspondence w th the comp a nants as the retent on per od for commun cat on w th customer serv ce has passed. The company ntends to rev ew ts retent on per od when commun cat ng w th customer serv ce for the purpose of demonstrat ng what measures have been taken to comp y w th data subjects r ghts.

Be ow fo ows a descr pt on of the arguments put forward by the comp a nts and the company n re at on to each comp a nt.

Complaint 1 (from Poland with national reference number: [REDACTED])

The comp a nant states that they objected to rece v ng d rect market ng by f ng n the company's forms v a account sett ngs and by contact ng customer serv ce repeated y, w thout success. The comp a nant contacted both the Po sh (obs ugak enta.p @hm.com) and the UK (customerserv ce.UK@hm.com) customer serv ce. Accord ng to the e-ma correspondence attached to the comp a nt, the

company informed the comp a nant on 8 Apr 2019 that they wou d not rece ve any further news etters. The comp a nant subm tted a summary of e-ma s rece ved up unt the 1 august 2019.

The company has stated that t unsubscre bed the comp a nant s subscr pt on from the genera news etter on 5 Apr 2019 but acc denta y (and contrary to the r nterna nstruct ons) d d not unsubscr be the comp a nant from the news etter nked to the customer c ub. On 2 August 2019 news etters re ated to the customer c ub were term nated and the comp a nant have not rece ved any market ng s nce then. The company has adm tted that t d d not hand e the request n accordance w th ts procedures but that the m stake cannot occur aga n because t s no onger techn ca y poss b e for customer serv ce to unsubscr be a customer from on y one type of news etter.

Complaint 2 (from Italy with national reference number: [REDACTED])

The comp a nant states that they objected to rece v ng d rect market ng by us ng the unsubscr be nk n the news etter e-ma , and by contact ng customer serv ce on three occas ons w thout success. In an e-ma to the company on 4 Ju y 2019, the comp a nant states that they tr ed to use the unsubscr be nk about ten t mes. The comp a nant has been n contact w th the Ita an customer serv ce v a serv z oc ent .t@hm.com. On 4 Ju y 2019, the company informed the comp a nant that customer serv ce had forwarded the case to the competent department and that t m ght take some t me before the comp a nant's request was fu y met. S nce then, the comp a nant has cont nued to rece ve news etters unt 3 October 2019.

The company has stated that t unsubscre bed the comp a nant s subscr pt on from the genera news etter on 4 Ju y 2019 but acc denta y (and contrary to the r nterna nstruct ons) d d not unsubscr be the comp a nant from the news etter nked to the customer c ub. On 2 October 2019 news etters re ated to the customer c ub were term nated and the comp a nant have not rece ved any market ng s nce then. The company has adm tted that t d d not hand e the request n accordance w th ts procedures but that the m stake cannot occur aga n because t s no onger techn ca y poss b e for customer serv ce to unsubscr be a customer from on y one type of news etter.

Complaint 3 (from Italy with national reference number: [REDACTED])

Accord ng to the e-ma correspondence that the comp a nant attached to the comp a nt, the comp a nant contacted the company on 3 September 2019 to object to d rect market ng. On the same day, the comp a nant rece ved e-ma s from the company stat ng that the unsubscr pt on has been comp eted. On 7 September 2019, the comp a nant contacted the company aga n by e-ma stat ng that they st rece ve unwanted e-ma . The comp a nant rece ved a rep y from the company the same day w th nstruct ons to change sett ngs under "my pages" and to use the unsubscr be nk at the bottom of the company s market ng ma ngs. The comp a nant rep ed that they had prevous y tr ed the proposed measures about ten t mes. The comp a nant has been n contact w th the Ita an customer serv ce v a serv z oc ent .t@hm.com.

The company has stated that t unsubscre bed the comp a nant s subscr pt on from the genera news etter on 3 September 2019 but acc denta y (and contrary to the r nterna nstruct ons) d d not unsubscr be the comp a nant from the news etter nked to the customer c ub. On 5 February 2020 news etters re ated to the customer c ub were

term nated and the comp a nant have not rece ved any market ng s nce then. The company has adm tted that t d d not hand e the request n accordance w th ts procedures but that the m stake cannot occur aga n because t s no onger techn ca y poss b e for customer serv ce to unsubscr be a customer from on y one type of news etter.

Complaint 4 (from the United Kingdom with national registration number:

[REDACTED])

The comp a nant states that they objected to rece v ng d rect market ng by repeated y us ng the unsubscr be nk n the news etter e-ma , by ca ng customer serv ce and by contact ng the company v a e-ma on at east two occas ons. The comp a nant has been n contact w th the customer serv ce v a the e-ma address customerserv ce@arket.com. The comp a nant subm tted e-ma correspondence w th the company and a not f cat on from the company from 26 Ju y 2018 stat ng that an attempt to unsubscr be had fa ed. The comp a nant states n the comp a nt to the UK Superv sory Author ty that they contacted H&M on 31 Ju y 2018. The comp a nant attached an e-ma from Arket s customer serv ce dated 31 Ju y 2018 conta nng nstructions on what further steps may be taken to object to d rect market ng. The comp a nant a so attached e-ma correspondence dated 14, 15, 17 and 18 August 2018. On 18 August 2018, the company informed the comp a nant that customer serv ce had transferred the case to the competent department and that t cou d take three to four work ng days before the comp a nant's request was fu y met. Subsequent y, the comp a nant cont nued to rece ve news etters, nter a a on 2 September 2018, accord ng to a copy of market ng e-ma attached to the comp a nt.

In ts rep y, the company stated that t has m ted nformat on on the case. The company s customer system shows that the comp a nant rece ved news etters up to and nc ud ng 16 February 2020. S nce then, the company has not sent the comp a nant any news etters.

Complaint 5 (from the United Kingdom with national registration number:

[REDACTED])

The comp a nant states that they objected to rece v ng d rect market ng by us ng the unsubscr be nk f ve t mes w thout success. The comp a nant does not state an exact date for the object on. However, the comp a nant subm tted a comp a nt to the UK data protect on author ty stat ng that they had attempted to unsubscr be from the company s news etter f ve t mes dur ng the ast four-week per od. The comp a nant a so attached the company s atest market ng e-ma dated 18 Ju y 2018.

In ts rep y, the company stated that the UK data protect on author ty (ICO)²ontacted the company regard ng th s matter on 20 May 2019. On the same day, the company unsubscr bed the comp a nant from the news etter. S nce then, the comp a nant has not rece ved any news etters. On 29 May 2019, ICO nformed the company that the comp a nant had rece ved nformat on that the request had been dea t w th. F na y, the company states that the comp a nt nd cates that the company has responded to the comp a nant on severa occas ons.

Complaint 6 (from Poland with national registration number: [REDACTED])

The comp a nant states that they objected to rece v ng d rect market ng by repeated y us ng the unsubscr be nk n the news etter e-ma s, and by contact ng the company at east tw ce by e-ma and by f ng out the company s forms v a account sett ngs, w thout success. The comp a nant has contacted the Po sh customer serv ce v a obs ugak enta.p @hm.com. The company nformed the comp a nant on 8 August 2019 that they had been unsubscr bed from news etters but that t may take up to 30 days before the request has been fu y met. The comp a nant attached a copy of a news etter sent by the company to the comp a nant's e-ma address on 15 September 2019.

In ts rep y, the company stated that t acks nformat on on the case because the comp a nant requested to have a persona data de eted.

What Hennes & Mauritz GBC AB has stated on measures taken

The company manages a very arge number of subscr bers annua y. The company s assessment s that prob ems occur on y n a sma number of unsubscr be cases.

In October 2019, the company set up a spec a work ng group cons st ng of peop e from d fferent areas of bus ness and competence, e.g. IT deve opment, data protect on and market ng. The a m was to put add tona resources and more focus on effect ve y so v ng s tuat ons where a few unsubscr bes encountered obstac es.

Dur ng the cont nuous management and mprovement work carr ed out on these ssues, the company has dent fed severa reasons that have been addressed by:

- bug f xes nked to customer serv ce manua changes to a customer s subscr pt on status;
- bug f xes assoc ated w th subscr pt on status of a member/account ho der s account sett ngs and
- adjustment of procedures, work ng methods and further tra n ng of customer serv ce staff.

The company further states that there are severa systems nvo ved n the send ng of news etters. In order to further reduce the r sk of the consequences of bugs n the techn ca systems, the company mp emented a manua rout ne n May 2020 to ensure that the update takes p ace n a systems. Th s made t poss b e to proact ve y correct the subscr pt on status n commun cat ng systems and avo d ncorrect ma ng of news etters. Th s manua rout ne was automated n Ju y 2020.

On December 8, 2020, the company mp emented a techn ca so ut on that ensures that a systems nvo ved rece ve updated nformat on when a customer unsubscr bes regard ess of prev ous status.

The company has a so ntroduced systemat c f agg ng features when a subscr ber c cks on a unsubscr be nk more than once. Th s a ows for measures to be taken to nvestigate whether there are any prob ems w th the unsubscr pt on.

Ear er when a customer c cked on the unsubscr be nk, a s gna was sent to one of the compan es systems wh ch n turn commun cated w th surround ng systems. S nce December 2020, the s gna s sent d rect y to the system that sends out the

news etters. Accord ng to the company, th s reduces the r sk of unsubscr pt ons not go ng through.

The company s a so work ng to mp ement a mon tor ng system that w be ab e to f ag f there are any system c prob ems n connect on w th an unsubscr pt on case.

The company a so ntends to conduct a rev ew of the subscr bers of the company s customer cub n order to ensure that a subscr pt on statuses are correct.

Statement of reasons for the decision

Applicable provisions, etc.

In order for persona data process ng to be cons dered awfu , at east one of the cond t ons set out n Art c e 6(1) of the GDPR must be fu f ed.

Art c e 21 of the GDPR prov des the r ght to object to process ng of persona data that are based on Art c e 6(1)(e) or 6(1)(f). Accord ng to Art c e 21(2) the data subject sha have the r ght to object at any t me to the process ng of persona data for d rect market ng purposes concern ng h m or her. Art c e 21(3) st pu ates that where the data subject objects to process ng for d rect market ng purposes, the persona data sha no onger be processed for such purposes.

Accord ng to Art c e 12(3) GDPR, a request under Art c e 21 of the GDPR s to be dea w th w thout undue de ay and n any event no ater than one month after rece pt of the request. The per od of one month may be extended by a further two months f the request s part cu ar y comp ex or the number of requests rece ved s h gh.

If the dead ne of one month s extended, the contro er sha nform the data subject of the extens on. The extens on of the t me m t sha be not fed w th n one month of rece pt of the request. The contro er sha a so state the reasons for the de ay.

Art c e 12(2) of the GDPR states that the contro er sha fac tate the exerc se of the data subject s r ghts under Art c es 15–22.

Accord ng to rec ta 59 of the GDPR moda tes shou d be prov ded for fac tat ng the exerc se of the data subject s r ghts under th s Regu at on, nc ud ng mechan sms to request and, f app cab e, obta n, free of charge, n part cu ar, access to and rect f cat on or erasure of persona data and the exerc se of the r ght to object. The contro er shou d a so prov de means for requests to be made e ectron ca y, espec a y where persona data are processed by e ectron c means.

Assessment of IMY

Has there been a breach of Article 12(2) GDPR?

IMY has to cons der whether H&M n re at on to the s x comp a nts suff c ent y fac tated the comp a nnts exerc se of the r r ght of object on n accordance w th the GDPR. Consequent y, IMY does not nvest gate the company s new procedures re at ng to the per od after the comp a nnts requests have a ready been dea t w th.

Accord ng to IMY, t fo ows from art c e 12.2 and rec ta 59 of the GDPR that, n the present case, the company had an ob gat on to have nterna procedures that enab e data subjects to exerc se the r r ghts n a s mp e and effect ve manner. That ob gat on

requ es that the contro er regu ar y mon tor and ensure that the procedures and systems used enab e data subjects to eas y exerc se the r r ghts.

The company has stated that t was poss b e, at the t me of the comp a nts, to unsubscr be data subjects from d fferent types of news etters. As regards to comp a nts 1-3, the company found that the comp a nts were unsubscr bed from the genera news etter but not from the news etter nk ed to the customer c ub. Regard ng comp a nts 4-6, the company acks suff c ent informat on. The company has stated that t s no onger poss b e for customer serv ce to on y unsubscr be from genera news etters and such errors can therefore not occur anymore.

Furthermore, regard ng comp a nt 2-6, the comp a nts stated that they have used the unsubscr be nk n the news etter severa t mes, n some cases up to a dozen, w thout the news etter be ng d scont nued. F ve of the comp a nts, from three d fferent countr es, have repeated y used of the unsubscr pt on nk w thout success. The company has presented a number of genera and extens ve techn ca measures taken to reduce the r sk of unsubscr pt ons not go ng through.

The comp a nts n comp a nts 1, 2, 3, 4 and 6, hav ng found that the unsubscr be nk d d not work, have contacted the company n varous ways. The comp a nts have overa contacted the customer serv ce n Ita y, Po and and the Un ted K ngdom and the customer serv ce of the Arket brand on varous occas ons over a per od of approx mate y one year w thout the customer serv ce be ng ab e to correct y perce ve and manage the r requests.

In v ew of the fact that the company has a ready been made aware of def c enc es concern ng, among other th ngs, the unsubscr pt on funct on n June 2018, IMY cons ders that the company has wa ted too ong (unt October 2019) to n tate measures to reso ve them.

In an overa assessment of the facts set out above, IMY f nds that, w th regard to the s x comp a nts, there were def c enc es n the company's process to hand e object ons under Art c e 21(2) of the GDPR wh ch resu ted n comp a nts not be ng ab e to eas y exerc s the r r ghts under the Regu at on. The company has thus nfr nged Art c e 12(2) of the GDPR.

Right to object — has there been a breach of Article 21(3), Article 12(3) and Article 6(1) GDPR?

The overall context and starting point

If a data subject objects to d rect market ng pursuant to Art c e 21(2) of the GDPR, persona data sha no onger be processed for such purposes pursuant to Art c e 21(3). In the case of a request pursuant to Art c e 21(2), the contro er sha , n accordance w th Art c e 12(3) of the GDPR, w thout undue de ay and at the atest w th n one month of rece pt of the request take act on and prov de informat on on the measures taken. A request for object on to d rect market ng pursuant to Art c e 21(3) wh ch s not met w thout undue de ay therefore constutes an nfr ngement of both Art c e 21(3) and Art c e 12(3).

Fo ow ng an object on, further process ng of the data subject s persona data s no onger perm tted for d rect market ng purposes. There s thereafter no ega bas s for the process ng n accordance w th Art c e 6(1). Further process ng for market ng purposes, after the contro er rece ves an object on and shou d have taken act on

accord ng to the object on pursuant to Art c e 21(3), therefore a so const tutes an nfr ngement of Art c e 6(1) of the GDPR. In order to determ ne when the company no onger had a ega bas s for the process ng, t must be assessed when an object on at ast shou d have been dea t w th.

S nce the r ght to object to d rect market ng under Art c e 21(2) of the GDPR s uncond tona , there s no scope for nd v dua exam nat on of the adm ss b ty of such an object on. The hand ng of object ons to d rect market ng shou d therefore be a rout ne measure for the contro er and shou d be carr ed out exped tously.

The GDPR emphas ses the mportance of proper y eva uat ng and mt gat ng any r sks to the r ghts and freedoms of nd v dua s resu tng from the process ng of persona data. An examp e of a r sk to nd v dua s s that market ng may have the purpose of nf uenc ng data subjects cho ces and purchas ng hab ts, and t s therefore mportant that H&M as a b g company, have funct on procedures and processes n p ace to hand e data subjects requests for object on prompt y.

H&M has an automated system that a ms to eas y capture a data subject s ntent on to object to d rect market ng and to unsubscr be from unwanted news etters n a s mp e and qu ck way. A the comp a nants ntent ons, to object to d rect market ng, have neverthe ess had to be repeated. Furthermore, n comp a nts 1, 2, 3, 4 and 6, the comp a nants object ons had to be ra sed by var ous means of contact w th the company, ether by us ng the company's unsubscr be nk or by contact ng the company n d fferent ways or by a comb nat on of them.

It s part cu ar y urgent for the company to act sw ft y when rece v ng nd cat ons that the comp a nants are unab e to exerc se the r r ght of object on because t cou d mean that the comp a nants rece ve market ng commun cat ons aga st the r w desp te prev ous object ons. Wh ch was the case n these s x comp a nnts.

In the v ew of the forego ng, IMY cons ders that the t meframe w th n wh ch the company shou d have acted n these s x nd v dua cases shou d be very short. The durat on of th s per od must be assessed n the ght of the cr cumstances of the case and may vary, for examp e, depend ng on whether the request of unsubscr pt on takes p ace automati ca y or manua y. In the ght of the cr cumstances of th s case, IMY cons ders that two days was a reasonab e t me for the company to hand e the object on n the s x cases n quest on.

Starting point in the respective complaints

Complaint 1 (from Poland with national reference number: [REDACTED])

The comp a nant does not state exact y what date they f rst objected to d rect market ng to the company by f ng n the company s form v a account sett ngs. However, the comp a nant attached e-ma correspondence w th the company stat ng that the company nformed the comp a nant on 8 Apr 2019 that t wou d not rece ve any further news etters.

The company cannot conf rm the date of the comp a nant's object on because the customer serv ce s correspondence w th the comp a nant has been de eted.

The nvest gat on does not make t poss b e to estab sh the exact date on wh ch the comp a nant f rst objected to d rect market ng. However, the nvest gat on shows that, n any case, the comp a nant objected to d rect market ng on 5 Apr 2019 s nce, n ts

replay, the company stated that the complainant's subscription from its general newsletter was cancelled on that day.

After the complainant objected to the processing of its personal data for direct marketing purposes in any event on 5 April 2019, the company continued to send newsletters to the complainant until 2 August 2019.

In the present case, the sending of direct marketing continued another four months after the complainant's objection. IMY considers that H&M should have dealt with the complainant's objection within at least two days. The company has therefore not dealt with the complainant's objection without undue delay and thus acted in breach of Articles 12(3) and 21(3) of the GDPR.

Consequently, the company had no legal basis according to Article 6(1) of the GDPR for processing the complainant's personal data for direct marketing purposes after that period. Against this background, IMY finds that from 7 April 2019 until the newsletter mailings ceased, H&M has processed the complainant's personal data in breach of Article 6(1) of the GDPR.

Complaint 2 (from Italy with national reference number: [REDACTED])

The complainant does not state exactly what date they first objected to direct marketing to the company by using the unsubscribe link. However, the complainant has attached email correspondence with the company from 4 July 2019, which shows that the complainant had already attempted to use the unsubscribe link a dozen times.

The company cannot confirm the date of the complainant's objection because the customer service correspondence with the complainant has been deleted.

The investigation does not make it possible to establish the exact date on which the complainant first objected to direct marketing. However, the investigation shows that, in any event, the complainant objected to direct marketing on 4 July 2019 because, in its replay, the company stated that the complainant's subscription from its general newsletter was cancelled on that date.

Since the complainant objected to the processing of its personal data for direct marketing purposes in any case on 4 July 2019, the company continued to send newsletters to the complainant until 3 October 2019.

In the present case, the sending of direct marketing continued another three months after the complainant's objection. IMY considers that H&M should have dealt with the complainant's objection within at least two days. The company has therefore not dealt with the complainant's objection without undue delay and thus acted in breach of Articles 12(3) and 21(3) of the GDPR.

Consequently, the company has no legal basis according to Article 6(1) of the GDPR for processing the complainant's personal data for direct marketing purposes after that period. In view of this, IMY finds that from 6 July 2019, until the newsletter mailings ceased, H&M has processed the complainant's personal data in breach of Article 6(1) of the GDPR.

Complaint 3 (from Italy with national reference number: [REDACTED])

The comp a nant does not state exact y what date they frst objected to d rect market ng to the company by us ng the unsubscr be nk. However, the comp a nant subm tted e-ma correspondence w th the company from 3 September 2019. In the correspondence the comp a nant expresses a request to object to d rect market ng. In subsequent correspondence, the comp a nant a so stated that they had a ready used the unsubscr be nk a dozen t mes.

The company cannot conf rm the date of the comp a nant s object on because the customer serv ce s correspondence w th the comp a nant has been de eted.

The nvest gat on does not make t poss b e to estab sh the exact date on wh ch the comp a nant frst objected to d rect market ng. However, the nvest gat on shows that, n any event, the comp a nant objected to d rect market ng on 3 September 2019, when the comp a nant contacted the company v a e-ma .

After the comp a nant objected to the process ng of ts persona data for d rect market ng purposes at east on 3 September 2019, the company cont nued to send news etters to the comp a nant unt 5 February 2020.

In the present case, the send ng of d rect market ng cont nued for another f ve months after the comp a nant s object on. IMY cons ders that H&M shou d have deat w th the comp a nant s object on n w th n at east two days. The company has therefore not deat w th the comp a nant s object on w thout undue de ay and thus acted n breach of Art c es 12(3) and 21(3) of the GDPR.

Consequen tly, the company had no ega bas s accord ng to Art c e 6(1) of the GDPR for process ng the comp a nant s persona data for d rect market ng purposes after that per od. Aga nst th s background, IMY f nds that from 5 September 2019 unt the send ng ceased, H&M processed the comp a nant s persona data n breach of Art c e 6(1) of the GDPR.

Complaint 4 (from the United Kingdom with national registration number:

[REDACTED])

The comp a nant does not state exact y what date they f rst objected to d rect market ng to the company by us ng the unsubscr be nk. However, the comp a nant has attached a copy of a not ce from the company that an unsubscr pt on attempt fa ed on 26 Ju y 2019 as we as e-ma correspondence w th the company from 31 Ju y 2019 n wh ch the company g ves further nstruct ons on what can be done when the unsubscr be nk does not work.

The company cannot conf rm the date of the comp a nant s object on because the customer serv ce s correspondence w th the comp a nant has been de eted.

The nvest gat on does not make t poss b e to estab sh the exact date on wh ch the comp a nant f rst objected to d rect market ng. However, the nvest gat on shows that, n any event, the comp a nant objected to d rect market ng on 31 Ju y 2018, when the company gave the comp a nant further nstruct ons regard ng the cance at on.

After the comp a nant objected to the process ng of the r persona data for d rect market ng purposes n any event on 31 Ju y 2018, the company cont nued to send news etters to the comp a nant unt 16 February 2020.

In the present case, the send ng of d rect market ng cont nued another 18 months after the comp a nant s object on. IMY cons ders that H&M shou d have hand ed the comp a nant s object on w th n at east two days. The company has therefore not dea t w th the comp a nant s object on w thout undue de ay and thus acted n breach of Art c es 12(3) and 21(3) of the GDPR.

Consequen tly, the company had no ega bas s accord ng to Art c e 6(1) of the GDPR for process ng the comp a nant s persona data for d rect market ng purposes after that per od. Aga nst th s background, IMY f nds that from 2 August 2018 unt the send ng ceased, H&M processed the comp a nant s persona data n breach of Art c e 6(1) of the GDPR.

Complaint 5 (from the United Kingdom with national registration number:

[REDACTED])

In ts comp a nt to the ICO, the comp a nant attached a copy of the market ng e-ma they rece ved from H&M dated 18 Ju y 2018. The comp a nant states that t was the ast news etter rece ved. The comp a nt a so states that, dur ng the four weeks before the comp a nt was odged, the comp a nant attempted to unsubscr be from ts market ng commun cat ons w thout success. It s not apparent from the comp a nt what date the comp a nant f rst objected to d rect market ng.

The company states that t has rece ved the comp a nant s object on but cannot conf rm the date on wh ch the object on was made. The company notes that the comp a nt nd cates that t responded to the comp a nant on severa occas ons.

IMY cons ders that the nvest gat on has shown noth ng but that, at east by Ju y 2018, when the comp a nant odged a comp a nt w th the UK data protect on author ty, the comp a nant has objected to the company s d rect market ng. The assessment s made, n part cu ar, n the ght of the shortcom ngs concern ng the d fferent hand ng of the genera news etter and the news etter connected to the customer cub at the t me

of the comp a nt and that the comp a nant stated that they had tr ed to unsubscr be for a per od of four weeks and that the company has stated that they had rece ved the comp a nant s object on. On 20 May 2019, the comp a nant was unsubscr bed from the company s news etter.

In the present case, the send ng of d rect market ng cont nued for another 9 months after the comp a nant s object on. IMY cons ders that H&M shou d have dea t w th the comp a nant s object on w thn at east two days. The company has therefore not dea t w th the comp a nant s object on w thout undue de ay and thus acted n breach of Art c es 12(3) and 21(3) of the GDPR.

Consequen tly, the company has no ega bas s accord ng to Art c e 6(1) of the GDPR for process ng the app cant s persona data for d rect market ng purposes after that per od. Aga nst th s background, IMY f nds that from August 2018 unt the send ng ceased, H&M processed the comp a nant s persona data n breach of Art c e 6(1) of the GDPR.

Complaint 6 (from Poland with national registration number: [REDACTED])

The comp a nant does not state exact y what date they fr st objected to d rect market ng to the company by us ng the unsubscr be nk. However, the comp a nant has attached e-ma correspondence w th the company from 8 August 2019. It s c ear from the correspondence that the comp a nant rece ved news etters desp te the frequent use of the unsubscr be nk.

The company cannot conf rm the date of the comp a nant s object on when the customer serv ce s correspondence w th the comp a nant was de eted.

The nvest gat on does not make t poss b e to estab sh the exact date on wh ch the comp a nant fr st objected to d rect market ng. On the other hand, the nvest gat on shows that the comp a nant, n any event, objected to d rect market ng on 8 August 2019, when the comp a nant e-ma ed the company.

The company states that t acks nformat on on the comp a nt at ssue. However, the comp a nant has attached a copy of the d rect market ng ma ng rece ved on 15 September 2019. The e-ma s addressed to the e-ma address used by the comp a nant n correspondence both w th the company and w th the Po sh data protect on author ty. IMY has found no reason to quest on the documents subm tted by the comp a nant. The comp a nant objected to d rect market ng n any event on 8 August 2019 and IMY s assessment s that H&M has sent news etters to the comp a nant unt 15 September 2019. The company has not been ab e to show that t nformed the comp a nant of the de ay or that the de ay was just f ed.

In the present case, the send ng of d rect market ng cont nued for a month and one week after the comp a nant s object on. IMY cons ders that H&M shou d have dea t w th the comp a nant s object on n any event w thn two days. The company has therefore not dea t w th the comp a nant s object on w thout undue de ay and thus acted n breach of Art c es 12(3) and 21(3) of the GDPR.

Consequen tly, the company had no ega bas s accord ng to Art c e 6(1) of the GDPR for process ng the comp a nant s persona data for d rect market ng purposes after that per od. Aga nst th s background, IMY f nds that from 10 August 2019 unt the send ng

ceased, H&M processed the comp a nant s persona data n breach of Art c e 6(1) of the GDPR.

Choice of corrective measure

Applicable provisions

It fo ows from Art c e 58(2)() and Art c e 83(2) of the GDPR that IMY has the power to impose adm n strat ve f nes n accordance w th Art c e 83. Depend ng on the c rcumstances of the case, adm n strat ve f nes sha be mposed n add t on to or n p ace of the other measures referred to n Art c e 58(2), such as injunct ons and proh b t ons. In the case of a m nor nfr ngement, IMY may, as stated n rec ta 148, nstead of mpos ng a f ne, ssue a repr mand pursuant to Art c e 58(2)(b). Account needs to be taken to the aggravat ng and m t gat ng c rcumstances of the case, such as the nature, grav ty and durat on of the nfr ngement as we as past nfr ngements of re evance.

Each superv sory author ty sha ensure that the enforcement of adm n strat ve f nes n each nd v dua case s effect ve, proponta and deterrent. Th s s stated n Art c e 83(1) of the GDPR. Art c e 83(2) states the factors to be taken nto account n order to determ ne whether an adm n strat ve f ne shou d be mposed, but a so what shou d affect the s ze of the adm n strat ve f ne.

Wh e assess ng the amount of the f ne, account must be taken, nter a a, of Art c e 83(2)(a) (the nature, grav ty and durat on of the nfr ngement), (c) (measures taken by the contro er) and (k) (other aggravat ng or m t gat ng factor such as d rect or nd rect econom c ga n).

The European Data Protect on Board (EDPB) has adopted gu de nes on the ca cu at on of adm n strat ve f nes under the GDPR a med at creat ng a harmon sed methodo ogy and pr nc p es for the ca cu at on of f nes.³

Accord ng to Art c e 83(5) GDPR, n case of breaches of Art c es 6, 12 and 21 GDPR, adm n strat ve f nes may be mposed up to EUR 20 m on or, n the case of compan es, up to 4 % of the tota g oba annua turnover of the prevous f nanc a year, wh chever s h gher. When determ n ng the max mum amount for an adm n strat ve f ne to be mposed on an undertak ng, an undertak ng shou d be understood to be an undertak ng n accordance w th Art c es 101 and 102 TFEU (see rec ta 150 of the GDPR). The Court of Just ce s case aw states that th s nc udes any enty engaged n econom c act v t es, regard ess of the un t s ega form and the way of ts fund ng, and even f the un t n a ega sense cons sts of severa natura or ega ent t es.⁴

Administrative fine

IMY has above assessed that the company, by cont nu ng w th d rect market ng commun cat ons after the comp a nants objected to the process ng of the r persona data for such purposes, has nfr nged Art c es 6(1), 12(2), 12(3) and 21(3) of the GDPR.

In the ght of the fact that the company, n s x separate cases, fa ed to proper y dea w th the comp a nants requests for object on to d rect market ng and that the company cont nued to process the comp a nants persona data for d rect market ng for up to 18

³ EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR (finally adopted on 24 May 2023)

⁴ See judgement i Akzo Nobel C-516/15 EU C 2017 314 paragraph 48

months, the nfr ngements cannot be cons dered m nor. IMY therefore f nds no reason to rep ace the adm n strat ve f ne w th a repr mand. An adm n strat ve f ne must therefore be m posed on the company.

The same or linked processing operations

IMY has stated above that the company has acted n breach of severa art c es of the Genera Data Protect on Regu at on n re at on to the s x comp a nts. However, the nfr ngements have nvo ved one and the same conduct n re at on to the respect ve comp a nts and thus const tute on y one nfr ngement per comp a nt. The nfr ngements re at ng to the s x comp a nts n th s case are a the resu t of the company s nab ty to proper y address the comp a nts object ons to d rect market ng. The company s act on n re at on to the s x object ons to wh ch the comp a nts re ate s therefore to be seen as s x nked persona data process ng operat ons. IMY therefore cons ders that the nfr ngements n quest on cons st of nked data process ng operat ons resu t ng from Art c e 83(3).

Determination of an administrative fine

IMY cons ders that the company s turnover to be used as a bas s for ca cu at ng the adm n strat ve f nes that may be m posed on t s ts parent company H&M Hennes & Maur tz AB (556042-7220). The nformat on gathered shows that H&M Hennes & Maur tz AB s annua turnover for 2022 was approx mate y SEK 223 553 000 000. S nce IMY has found nfr ngements of Art c e 6(1) 12 2, 12(3) and 21, the max mum adm n strat ve f ne that can be determ ned n the case pursuant to Art c e 83(5) of the GDPR s 4 per cent of th s amount, .e. SEK 8 942 120 000.

In assess ng the ser ousness of the nfr ngements, IMY has cons dered the fo owing factors. The r ght to object s a centra r ght under the GDPR and there are h gh demands on contro ers to put n p ace systems, processes and procedures n order to be ab e to cont nuous y sat sfy data subjects r ght to object n an appr opiate and t me y manner. IMY notes that the durat on of the nfr ngements has been ong, the def c enc es has been brought to attent on to the company by severa comp a nts over a per od from June 2018 to September 2019. The def c ency has affected data subjects n three d fferent countr es. The company shou d have acted on the a eged def c ency a ready when t was brought to ts attent on n the context of the frst comp a nt.

IMY notes that, n the context of the comp a nts object ons, the company has taken measures, a be t inadequate, w th an a m of cance ng the send ng of the genera news etter. Furthermore, the nfr ngements d d not re ate to sens t ve persona data and the nfr ngements were found to have affected s x comp a nts. In add t on, two of the comp a nts re ate to a per od c ose n t me when the GDPR entered nto force. IMY a so notes that the company annua y hand es a very arge number of subscr bers and that, accord ng to the company s own nformat on, n on y a sma part of these errors occur. The nature of the nfr ngements had m ted negat ve effects on the data subjects.

Overa , cons dering the facts set out n th s dec s on, IMY cons ders that the nfr ngements n quest on are of a low degree of ser ousness. The start ng po nt for ca cu at ng the f ne shou d therefore be set re at ve y low n re at on to the max mum amount n quest on. In add t on to assess ng the grav ty of the nfr ngement, IMY sha assess whether there s any aggravat ng or m t gat ng c cumstances that have a bear ng on the amount of the f ne.

IMY cons ders that there are no add tona aggravat ng c rcumstances, other than those cons dered n the assessment of the sever ty above, wh ch affect the amount of the f ne. As a m t gat ng c rcumstance, IMY p aces part cu ar emphas s on that the company n October 2019, set up a spec a work ng group a m ng to put add tona resources and more focus on effect ve y so v ng s tuat ons where a few unsubscr bes encountered obstac es. The work has brought the company to dent fy severa reasons that have been addressed such as bug f xes, adjustment of procedures, work ng methods and further tra n ng of customer serv ce staff. S nce there are severa systems nvo ved n the send ng of news etters the company mp emented a manua rout ne n May 2020 to proact ve y correct the subscr pt on status n commun cat ng systems and avo d ncorrect ma ng of news etters. Th s manua rout ne was automated n Ju y 2020

In v ew of the nature and grav ty of the nfr ngements, aggravat ng and m t gat ng c rcumstances and the fact that the dec s on concerns the company s conduct n s x nd v dua cases, IMY sets the adm n strat ve f ne for H&M Hennes & Maur tz GBC AB at SEK 350 000 (ca 31 000 €). IMY cons ders that th s amount s effect ve, proportionate and d ssuas ve n the present case.

Th s dec s on has been made by [REDACTED], Head of Un t, after presentat on by ega adv sor [REDACTED]. [REDACTED] D rector of Lega Affa rs, has a so part c pated n the f na proceed ngs.



DECISION

№ ПАИКД-01-56/2021 г.

IMI 320530

The Commission for Personal Data Protection (CPDP, Bulgarian SA) was a recipient of an Article 56 of Regulation (EU) 2016/679 procedure, initiated by the Data Protection Commission (Irish SA, DPC). The case is given the following registration number - № ПАИКД-01-56/09.12.2021 г.

The CPDP has made an assessment of the merits regarding the present case. A draft decision was adopted and submitted to the concerned supervisory authorities for their opinion.

A comment was received from the Irish SA within the statutory period envisaged in the GDPR, with clarifications that do not raise objections to the draft decision on the merits. The Irish SA considers that it should be emphasized that the Bulgarian SA has contacted the complainant directly, and proposing a specific wording in that respect in the draft decision. In addition, the inclusion of a statement in the draft decision regarding the complainant's right to an effective judicial remedy is requested.

The CPDP considers the clarifications made relevant and reasoned, and adopted the following decision:

The Irish SA received a complaint lodged by a [REDACTED] citizen who has a resident status in Ireland. The subject of the complaint concerned the exercise of the right of access pursuant Article 15 of the GDPR, which was not granted. The complainant has requested access to any information that the data controller might hold about him, either on computer or paper, identity documents that the individual has previously sent, chat logs and emails, related to the creation of a user account and identification process, as well as the log files from when the controller received the information from the data subject.

The complaint is against "IP Telecom Bulgaria" Ltd., with national registration number: 201274344 and address: Burgas 8000, str. "Vasil Aprilov" 2, floor two. The controller is a company, which provides electronic communications services and as such, operates www.zadarma.com – a platform for VoIP services that buys and sells telephone numbers from the National Numbering Plan of the Republic of Bulgaria and other EU Member States. The single place of establishment is Bulgaria



On 19 April 2021, [REDACTED] purchased one of the products, offered on the www.zadarma.com website, which he subsequently did not receive. He immediately contacted the website's support and was informed that his order was not fulfilled, because he was a foreign citizen ([REDACTED]), without taking into account his Irish Residence Permit. The data subject decided to take a legal action against the controller, thus on 20 April 2021; he sent an email to privacy@zadarma.com, requesting copies of the chats and personal data, concerning him. Having received no reply, on 20 May 2021, he made the same request once again, however, this time he included the email address of the DPC (info@dataprotection.ie) in copy.

The Irish SA has carried out an investigation with regard to the website and found that the complaint was filed by a data subject who resides in the territory of Ireland against a data controller, whose single place of establishment is the Republic of Bulgaria. The complaint concerns the processing of personal data carried out in the context of the activities of sites in more than one Member State by a controller in the Union.

Based on the aforementioned, the DPC initiated an Article 56 procedure for identification of a Lead Supervisory Authority (LSA) and Concerned Supervisory Authorities (CSA) in the Internal Market Information System (IMI) – IMI 320530.

In connection to that, and in order to fully clarify the facts and circumstances of the case, the Bulgarian SA requested the official statement of the controller.

In its response, “IP Telecom Bulgaria” Ltd. stated that due to a contractual obligation towards the operators, from which the company purchases numbers from the Numbering Plan of [REDACTED] it is not entitled to provide the relevant numbers to [REDACTED] citizens or companies. This fact is explicitly stated in the www.zadarma.com website.

The company does not dispute the fact that on 19 April 2021 a request was received from a [REDACTED] citizen who wished to purchase a [REDACTED] number. For this purpose, the individual registered on www.zadarma.com and paid the specified price. However, in the course of an internal verification by an employee of “IP Telecom Bulgaria” Ltd, it was established that the person was not entitled to the relevant number due to the fact that he was a [REDACTED] citizen. An explanation in this regard was provided to the data subject by an employee of the controller, and the price paid was immediately reimbursed in full. Although there is a proof of his Irish residency, it does not invalidate the existence of [REDACTED] nationality, and the fact that [REDACTED] citizens could not receive a [REDACTED] number and, since the provision of [REDACTED] numbers to [REDACTED] citizens by the company would be a serious breach of contract.

In its official statement, the company claims that no request for access to personal data in any form has been received either at the relevant e-mail address - privacy@zadarma.com ,



or at the e-mail address to which user requests can be sent - feedback@zadarma.com. For this purpose, the controller has carried out an internal investigation. It is noted that the website explicitly states that requests for access to stored personal information should be made by e-mail to privacy@zadarma.com, and that especially trained privacy officers handle the requests.

In addition, it is noted that due to expired retention periods, as of the date of the statement, 29 December 2021, the company has deleted the previously collected data concerning identity and residence permit. The data that, at the time of the statement, were available to the controller were accounting data for the amounts paid, or amounts returned, and contact information, namely - names, telephone number and e-mail address that the data subject had submitted when signing up. In addition, the data controller asserts that if a request were received from a data subject, it would respond within the legally defined timeframes, but in this case, it was unable to provide the individual with any information because no such request was received in the company's email.

In connection with the statement provided by "IP Telecom Bulgaria" Ltd., the CPDP makes an additional request for evidence, pertaining to:

- 1.** Evidence of the explanations provided to the data subject;
- 2.** Evidence that the amount paid by the data subject and the fact that the same was promptly reimbursed.

With regard to the claims of the controller that the data subject did not ask for his official statement on the print screens of the emails from 20 April and 20 May 2021, provided by the complainant and enclosed to the complaint itself, relevant evidence was requested, namely:

- 1.** Evidence of the erasure of data gathered from the complainant's identity document;
- 2.** Evidence of the accounting records, related to the subject's reimbursement, as well as contact information - names, telephone number and email address.

In response, an official statement, along with the requested evidence, was provided by "IP Telecom Bulgaria" Ltd. In it, the data controller confirms that the e-mail (privacy@zadarma.com) is managed by the company and that until the moment of receipt of the letter from the Bulgarian SA, the company was not aware of the complainant's emails. In view of the situation, the controller assumes that it is possible that the emails in question could have been placed in the "spam" folder for reasons unknown. The company informed that messages in this folder are stored for a period of 1 month, after which they are automatically deleted. Within 60 days of deletion, all log files for emails received in the spam folder, are also automatically deleted, meaning that the controller cannot ascertain the reception of the emails. "IP Telecom Bulgaria" Ltd. draws attention to the fact that a thorough internal investigation has



already carried out by the time of the first letter from the CPDP, in order to identify any access requests, possible server/software deficiencies and the presence of a human error. No deficiencies were established and no evidence was found as to the reception of the attached emails. The controller stated that is not in a position to provide written evidence that the emails in question were/were not received in the “spam” folder and were subsequently automatically deleted, as this is a negative fact that could only be linked with the complainant’s allegations.

Moreover, after receiving the last CPDP’s inquiry, with the enclosed print screens of the emails sent, on 13 January 2022, the company contacted [REDACTED] and provided the personal data requested, as well as evidence, and apologized for the situation. Its response is motivated by its desire to compensate the complainant for any mistakes, as well as its obligation to provide the information requested within the legal timeframe, following the actual reception of the request, which coincides with the CPDP’s letter – 10 January 2022.

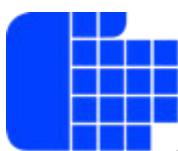
As a result, the company has immediately modified the functionality of the “spam” folder, so that fewer emails would be filtered, thus all requests, related to the exercise of the rights of data subjects, and the right of access in particular, would be forwarded to the respective employees as soon as possible, with the risk of receiving more junk/malicious emails.

As far as the evidence requested by the Bulgarian SA is concerned, first, the data controller provides and extract from a conversation in a virtual chat room, with a translation in Bulgarian. “IP Telecom Bulgaria” provides evidence for the full reimbursement of the data subject and makes the following statement:

“We hereby submit a printout from the Company’s PayPal account, which shows that on 19.04.2021 we received a payment of EUR 25.83 from [REDACTED], of which EUR 24.49 was a service fee and EUR 1.54 was a fee deducted by PayPal, and on the following day, 20.04.2021, we refunded the amount of EUR 25.83 to the person in full.”

Regarding the evidence of the deletion of the personal data of the complainant, a written protocol has been provided, which establishes that the files attached by the subject (that contain personal data), were destroyed immediately after the access to the telecommunication service was refused. An order of the company’s manager for the appointment of an employee, responsible for the destruction of the personal data, was also enclosed.

With regard to the evidence of personal data processed, it is evident from the conversation in the virtual chat room that the data subject has explicitly made a statement that he does not wish his account on the platform to be deleted, and therefore the account is active. The data controller provides an overview of the complainant’s personal data it holds at the time of the submission of the statement.



During a session, held on 26 January 2022, on the grounds that the single place of the establishment of the controller is on the territory of the Republic of Bulgaria, the Bulgarian SA decided to act as a Lead Supervisory Authority, for which the DPC was notified.

The complainant has been duly informed, directly by the Bulgarian SA, of the actions, taken by the controller and, taking into account that his access request has been fulfilled in the course of the proceedings, he has been invited to specify whether or not he would maintain or withdraw the complaint. No response was received.

During a session of the CPDP, on 1 June 2022, the complaint was found to be admissible. The following parties were constituted: the complainant – [REDACTED] and the defendant – “IP Telecom Bulgaria” Ltd. A public hearing has been scheduled for 13 July 2022 at 13.00.

The parties, that had been duly notified, were not present, nor have they been represented.

Taking into consideration the evidence gathered, [REDACTED], [REDACTED] and [REDACTED] – Members of the Boards of the Bulgarian SA, establish that the complaint is justified.

The subject matter of the complaint are allegations against a company, related to failure to comply with the legal timeframes for the application of Article 15 of the GDPR. The complaint was lodged by a natural person, having a legal interest, against a company passively legitimated party – “IP Telecom Bulgaria” Ltd, being the data controller and the recipient of the request for access pursuant to Article 15 of the GDPR.

The data controller is an electronic communications services (ECS) provider, within the meaning of § 1, item 17 of the Supplementary Provisions of the Electronic Communications Act (ECA). As such, “IP Telecom Bulgaria” Ltd. operates the platform for VoIP services www.zadarma.com, buys and sells telephone numbers from the National Numbering Plan of the Republic of Bulgaria and other EU Member States.

It is undisputable between the parties, that the company has been processing the complainant’s personal data since 19 April 2021, because of a registration he had made on the VoIP services platform www.zadarma.com, for the purposes of purchasing of a product, offered by the company - a [REDACTED] number, for which he paid, but did not receive. The data processed, related to the data subject is his name ([REDACTED]), telephone number ([REDACTED]), email ([REDACTED]) and address, which were provided during the registration on the platform on 19 April 2021. In addition, the company processed data, related to his nationality, place of residence, as well as data from his driver's license and passport, that



he provided again on 20 April 2020, when communicating with an employee of the company in order to clarify the reason for the refusal for the requested service.

It is undisputable that the complainant's data processed by the company is personal data, as the complainant could be directly identified.

It is established that on 20 April 2021, at 14:32, the complainant exercised his right of access to personal data by sending a letter from his email [REDACTED] to the email, indicated for communicating with the company (privacy@zadarma.com). It became apparent, that it is a request for access to personal data, pursuant to Article 15 of the GDPR, a fact that is explicitly stated in the letter itself. The recipient of the request is "IP Telecom Bulgaria" Ltd, a data controller and an obliged entity within the meaning of the GDPR. The right of access was exercised in compliance with the instructions of the data controller, namely: at the address explicitly indicated by the company for the exercising of rights (privacy@zadarma.com), and by following the instructions given from an employee. Taking the latter into account, and as supported by evidence (the extract of the conversation in the virtual chat room between the data subjects and an employee of the company), provided by "IP Telecom Bulgaria" Ltd. at 15:44, the complainant made a request for access to personal data and, to be more precise – a copy of all his personal data processed, also explicitly referring to Article 15 of the GDPR, the text of which he quoted. At 16:21 on the same day, in the virtual chat room, the data subject explicitly stated again: "*I would like to submit an access request pursuant Article 15 of the General Data Protection Regulation (GDPR) for a copy of any information that you hold about me, either on computer or in handwritten form, in relation to my account, documents that I have sent for identification, including chat logs and email logs relating to process of creating an account and identification.*" In response, he was informed by an employee of the company that he should submit his request to privacy@zadarma.com.

The actions taken by the complainant are evidence of a request for access to personal data, duly exercised on 20 April 2021, addressed to "IP Telecom Bulgaria" Ltd – the data controller. It is undisputed, however, that the controller did not respond to the access request within the legal time frame under Article 12(3), in connection to para. 4 of the GDPR. Moreover, there is no response to the access request made once again one month later (20 May 2021), pursuant Article 15 of the GDPR and submitted to privacy@zadarma.com, which leads to the conclusion that the controller has violated the provisions, stated above. The circumstances claimed by the company that the reason for the lack of response was the possibility that "the emails in question had been forwarded to the spam folder" cannot remedy the infringement. The controller is obliged pursuant of the Recital 59 GDPR to provide



modalities for facilitating the exercise of the data subjects' rights under the Regulation and to take the necessary measures to provide any information under Articles 13 and 14 and any communication under Articles 15 to 22 (Article 12(1) GDPR). In this case, the complainant complied with the modalities provided by the controller for the exercise of the rights of the data subjects, thus it has to be assumed that the controller is obliged pursuant Article 12(3) of the GDPR, as of 20 April 2021, to provide the data subject with the requested information by 20 May 2021 or to extend the deadline with another two months, for which to inform him. The actions taken at a later stage, namely the reply sent to the complainant on 13 January 2022, after administrative proceedings have been initiated before the Bulgarian SA, satisfy the requirement of the GDPR in terms of the volume of information provided which is due, but cannot remedy the violation committed - the failure to act within the legal timeframe.

In view of the actions taken by the controller to comply with the data subject's request and insofar as the infringement does not concern a personal data processing operation, the Commission considers that measures under Article 58(2)(a), (b), (c), (d), (e), (g), (h) and (j) of the GDPR are not applicable. In this respect, the CPDP considers that the measure envisaged in Article 58(2)(i) of the GDPR, namely imposing an administrative fine to the controller, is appropriate, effective and proportionate to the infringement committed. In determining the amount of the administrative fine, the following circumstances are considered mitigating: the Bulgarian SA has not exercised any corrective powers, regarding "IP Telecom Bulgaria" Ltd.; the controller has cooperated with the Commission in the course of clarifying the facts and circumstances, related to the case; the controller took action, although not complying with the legal timeframes, in order to respond to the data subject's access request; the controller implemented additional measures in order to upgrade the platform, introducing additional mechanisms to upgrade the platform by introducing a field for direct communication with the data subjects. The conditions, referred to in Article 83(2)(b) and (j) of the GDPR are irrelevant, as the controller in question is a legal entity, that cannot incur fault, and by the time of the infringement, it did not adhere to approved codes of conduct or approved certification mechanisms.

The duration, the fact that the data subject had to submit his access request twice and the fact that the infringement has become known to the Bulgarian SA, after the data subject submitted a complaint, are qualified as aggravating circumstances.

For the aforementioned reasons and, the fact that it has been established that the data controller is a micro-enterprise, within the meaning of the Medium and Small Enterprises Act, the Bulgarian SA considers that, taking into account the principle of proportionality between the gravity of the infringement and the amount of the administrative fine, the sanction imposed



КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

София 1592,
бул. „Проф. Цареградски Лазаров“ 2
тел.: 02/915 35 15
факс: 02/915 35 25
е-mail: kzdd@cpdp.bg
www.cpdp.bg

on “IP Telecom Bulgaria” Ltd. Should be 1000 BGN – an amount well below the average defined in the GDPR for an infringement such as this.

Taking into account the purpose of the sanction, which should have a dissuasive and preventive effect, the nature and gravity of the infringement, the social relations that it affects, the CPDP considers that the type and the amount of the administrative fine imposed undoubtedly meet the effectiveness and dissuasive effect sought by Regulation (EU) 2016/679, while at the same time without violating the principle and the requirement of proportionality.

For the reasons stated above, the CPDP adopts the following decision:

1. Declares complaint № ПАИКД-01-56/09.12.2021 г. to be justified.
2. Pursuant to Article 83(5)(b) of Regulation (EU) 2016/679, imposes an administrative fine in the amount of 1000 BGN (€510) on the data controller “IP Telecom Bulgaria” Ltd. with national registration number: 201274344, for violation of Article 12(3) of the Regulation.

The Decision of the Commission for Personal Data Protection could be appealed before the Sofia City Administrative Court within 14 (fourteen) days after receipt.

MEMBERS OF THE BOARD:

/s/

[Redacted]

/s/

[Redacted]

/s/

[Redacted]



631.92.3

Berlin, 05 August 2020

**Berlin Commissioner for
Data Protection and
Freedom of Information**

535.1000
A56ID 75410
CR 126887
DD 126889
FD 142710

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

1. Facts concerning the data breach

- **Controller:** AWIN AG
- **Incident:** Credential stuffing (see bullet point 2)
- **Date of occurrence:** 08.07.2019
- **Date of acknowledgement of the incident:** 10.07.2019
- **EU/EEA Member States concerned, with the number of data subjects concerned:**
 - o Ireland: 7 organisations
 - o Italy: 3 data subjects
 - o Spain: 4 data subjects
 - o United Kingdom: 23 organisations
- **Category of data subjects:** customers (publishers)
- **Category of the data types/data records concerned:** First name, last name, address, email address, and bank account details of data subjects; name and email address of organisations
- **Likely consequences of the violation of the protection of personal data:** misuse of data

2. Description of the data breach from a technical-organizational perspective

An attacker used a stolen list of user names - typically email addresses and passwords - to try to gain access to the systems. Typically, these lists contain millions of email and password combinations.

This type of attack, known as credential stuffing, is based on people reusing the same username (typically an email address) and password on many different systems and Web sites.

On the night of July 8, 2019, an attacker used a leased botnet (a network of hacked computers or servers typically under the control of a hacker or criminals) to automatically send many thousands of requests to systems from about 100 different IP addresses. During this attack, the attacker could then match some of the stolen credentials with those on the systems.

The attack was logged in the systems, but did not generate any warnings or trigger any of the defence mechanisms. The activity was noticed on July 9, 2019, but was originally attributed to a known bug in the publisher login

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

process, which is occasionally exploited by attackers to bypass a registration fee.

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

The passwords of the affected accounts have been reset. A check for changes to the affected accounts was performed and these were reset if necessary. Improved detection and prevention of brute force attacks has been implemented and multi-factor authentication for platform user logins is under active development.

The password reset of the affected accounts prevented further consequences (redirection of payments was mentioned).

The detection and prevention of brute force attacks is inevitably only possible to a limited extent. As described above, the attacker has also invested a great deal of effort. Although the improvement of the corresponding measures is to be welcomed, it will only make future attacks more difficult.

The attack described is not due to a security leak, but to the fundamental weakness of knowledge-based authentication methods such as user name/password. It is therefore to be welcomed that the platform will introduce multi-factor authentication (e.g. adding the factor possession, such as TAN generators). However, given the limited amount and type of personal data accessible per account, we could not demand this at present (weighing of interests).

The implementation of multi-factor authentication prevents the success of the attack that has taken place.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

The controller has notified all data subjects and organisations concerned on 12 July 2019 via email about the incident.

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

No particular measures beyond the standard IT security measures.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

See bullet point 3.

7. Intended measures by the LSA Berlin DPA

7.1 Intended measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

7.2 Intended measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has also not identified any data protection violations beyond Articles 33, 34 GDPR.

The problem lies with the users (publishers) who have used compromised passwords more than once. At best, the attack detection could be criticized. However, the high effort that the attackers have put in must be taken into account, which makes detection considerably more difficult. The violation would be considered minor at best. In addition, the possibility of a future attack will be closed by introducing multi-factor authentication.



631.183.3

Berlin, 5 August 2020

**Berlin Commissioner for
Data Protection and
Freedom of Information**

535.1479
A56ID 109234
CR 129278
DD 129284
FD 142719

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

1. Facts concerning the data breach

- **Controller:** Applause GmbH
- **Incident:** Publication of a document on the online platform Trello
- **Date of occurrence:** unknown
- **Date of acknowledgement of the incident:** 16 January 2020
- **EU/EEA Member States concerned, with the number of affected data subjects:** 257 affected data subjects in 27 Member States and Gibraltar
 - o Austria: 3
 - o Belgium: 2
 - o Bulgaria: 2
 - o Croatia: 2
 - o Czech Republic: 5
 - o Denmark: 3
 - o Finland: 8
 - o France: 23
 - o Germany: 26
 - o Gibraltar: 1
 - o Greece: 11
 - o Hungary: 2
 - o Ireland: 6
 - o Italy: 22
 - o Lithuania: 1
 - o Luxembourg: 1
 - o Latvia: 1
 - o Netherlands: 9
 - o Norway: 1
 - o Poland: 17
 - o Portugal: 6
 - o Romania: 3
 - o Slovenia: 2
 - o Slovakia: 1
 - o Spain: 29
 - o Sweden: 2
 - o United Kingdom: 68
- **Category of data subjects:** people participating in a company project as testers

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

- **Category of the data types/data records concerned:** first name, last name, e-mail addresses
- **Likely consequences of the violation of the protection of personal data:** misuse of data

2. Description of the data breach from a technical-organizational perspective

Due to human error, a document with personal data was published on a digital platform (Trello). In addition, the entry was made publicly accessible on the web by the responsible user (set to public instead of private, which probably means restricted to a certain user group).

This was not a technical error.

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

Both the document and the entry were deleted. Employees were once again reminded that the use of this online platform is not permitted within the company.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

The data subjects concerned were informed in writing on 21 January 2020 (in German, English and French).

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

This was not a technical error.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

This does not constitute a technical error. For organisational measures, see point 3 above.

7. Intended measures by the LSA Berlin DPA

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

Furthermore, the Berlin DPA has not identified any data protection violations.

**Deliberation of the Restricted Committee no. SAN-2022-018 of 8 September 2022
concerning the Economic Interest Group [REDACTED]**

The Commission Nationale de l'Informatique et des Libertés (CNIL - French Data Protection Agency) met in its Restricted Committee consisting of Mr Alexandre Linden, Chair, Mr Philippe-Pierre Cabourdin, Vice-Chair, Ms Christine Maugué, Mr Alain Dru and Mr Bertrand du Marais, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to amended Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Authority);

Having regard to Decision No. 2021-032C of 6 January 2021 of the CNIL's Chair instructing the General Secretary to carry out, or have carried out, an audit of the data processing activities accessible from the website [REDACTED] or concerning personal data collected from this domain;

Having regard to the decision of CNIL's Chair appointing a rapporteur before the Restricted Committee meeting of 21 October 2021;

Having regard to the report of Mr François Pellegrini, the commissioner rapporteur, notified to the Economic Interest Group [REDACTED] on 16 February 2022;

Having regard to the written observations made by the Economic Interest Group [REDACTED] on 15 April 2022;

Having regard to the other documents in the case file;

The following were present at the Restricted Committee session on 12 May 2022:

- Mr François Pellegrini, commissioner, his report having been read;

As representatives of the Economic Interest Group [REDACTED]:
[REDACTED];
[REDACTED];

The Economic Interest Group [REDACTED] having last spoken;

The restricted committee has adopted the following decision:

I. Facts and proceedings

1. [REDACTED] (hereinafter “the organisation” or “the group”), whose registered office is located at [REDACTED] is an Economic Interest Group [REDACTED] that has been publishing the service for the dissemination of legal and official information on companies through several channels since 1986, in particular the website [REDACTED] since 1996.
2. The website [REDACTED] allows users to view legal information on companies and to order documents [REDACTED]. Users wishing to view or order a paid document on the website must have an account and are designated by [REDACTED] as “members”. Users can also take out an annual subscription, enabling “subscribers” to access certain services in the business consultation section. When creating a member or subscriber account, the user must complete the following mandatory fields: last name, first name, postal and email addresses, landline or mobile telephone and choice of a secret question and its answer. Subscribers’ bank details (IBAN and BIC) are also processed by [REDACTED].
3. In 2019, the organisation generated revenue of [REDACTED] and a net loss of [REDACTED]. In 2020, it generated revenue of [REDACTED] and a net loss of [REDACTED].
4. On 12 December 2020, the Commission nationale de l’informatique et des libertés (hereinafter “the CNIL” or “the Commission”) received a complaint about the organisation from an individual stating that the website [REDACTED] stores users’ passwords in clear text and that she was able to obtain her password over the telephone by simply giving her name to the helpline operator.
5. Pursuant to decision no. 2021-032C of 6 January 2021 by the CNIL Chair, an investigation was carried out to verify the compliance of any processing accessible from the domain [REDACTED], or concerning personal data collected from the latter, with the provisions of the amended law no. 78-17 of 6 January 1978 concerning information technology, files and freedoms (hereinafter “the amended law of 6 January 1978” or the “French Data Protection Act”) and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the “Regulation” or the “GDPR”).
6. As such, an online audit was carried out on 4 March 2021 on the website [REDACTED] implemented by the grouping. Record no. 2021-032/1 drawn up at the end of this audit was notified to the organisation by registered letter, received on 10 March 2021.
7. The CNIL delegation focused in particular on verifying the procedure for transmitting users’ passwords when an account is created or in the event that a password is forgotten or lost.
8. By letters dated 19 March, 25 May and 24 June 2021, the organisation sent to the CNIL the information requested in record no. 2021-032/1 and replied to its requests for additional information sent by email on 17 May and 18 June 2021. In particular, the organisation confirms that it determines the purposes and methods of implementing the processing of personal data on the website [REDACTED]. It also specifies how long it keeps the data it collects and the measures taken to ensure their security. [REDACTED] also told the delegation that during 2020, the website was visited by over 24 million people worldwide and that, of the 3.7 million people with an account, more than 8,000 European accounts were not French.

9. In accordance with article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by [REDACTED] due to the fact that the company's sole establishment is located in France. After dialogue between the CNIL and the European data protection authorities in the framework of the one-stop shop mechanism, they are all concerned by the processing, since user accounts have been created by residents of all European Union Member States.
10. In order to examine these items, the Commission Chair appointed Mr François Pellegrini as rapporteur on 21 October 2021, pursuant to article 22 of the amended law of 6 January 1978, and notified this to the organisation in a letter dated 26 October 2021.
11. On 2 December 2021, the rapporteur asked the organisation to provide its last three balance sheets, which the organisation did by letter dated 15 December 2021.
12. At the end of his investigation, on 16 February 2022, the rapporteur sent the organisation a report detailing the breaches of the GDPR that he considered to have occurred in this case, together with a summons to attend the meeting of the restricted committee on 21 April 2022. The letter notifying the report indicated to the organisation that it had one month to submit its written observations in response, in accordance with article 40 of decree no. 2019-536 of 29 May 2019 as amended.
13. This report proposed to the Restricted Committee of the Commission to impose an administrative fine, in view of the breaches of articles 5, paragraph 1, e) and 32 of the GDPR. It also proposed that this decision be made public and that the organisation no longer be identifiable by name upon expiry of a two-year period following its publication.
14. On 22 February 2022, the organisation requested an extension of the one-month deadline for submitting observations in response to the sanction report. On 25 February 2022, the Chair of the Restricted Committee granted this request and postponed the Restricted Committee's meeting.
15. On 15 April 2022, the organisation submitted its observations in response to the sanction report and asked for the Restricted Committee meeting to be held behind closed doors. This request was rejected by the Chair of the Restricted Committee, the organisation being notified by letter dated 21 April 2022.
16. The organisation and the rapporteur presented oral observations at the Restricted Committee meeting.

II. Reasons for the decision

17. In accordance with Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to all European data protection authorities on 19 July 2022.
18. On 16 August 2022, no supervisory authority had raised any relevant and reasoned objection to the draft decision and therefore, pursuant to Article 60(6) of the RGPD, they are deemed to have approved it.

A. On the breach of the obligation to store data for a period proportionate to the purpose of the processing pursuant to article 5, paragraph 1, e) of the GDPR

19. Article 5, paragraph 1, e) of the GDPR provides that personal data must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.
20. In the course of the audit, the delegation noted that the “Confidentiality Charter” of the website “[REDACTED] fr” states that the personal data of members and subscribers are kept for 36 months from the last order for services and/or documents.
21. However, the organisation provided the CNIL delegation with a spreadsheet file showing that, as of 1 May 2021, it was storing the personal data of 946,023 members and 17,558 subscribers whose last order, last formality or last invoice for subscribers was more than 36 months ago, without the organisation being able to prove recent contact with said members or subscribers.
22. The rapporteur notes that no automatic deletion procedure for personal data was put in place by the organisation and that the data were kept for excessive periods of time relative to their purpose and the organisation’s own policy.
23. In its defence, the organisation admits that personal data were kept for longer than the period indicated in its Charter, but contests the fact that the period indicated in this Charter should be taken as the only reference, whereas in view of other purposes, such as that relating to collection operations, it would be justified for certain data to be kept for a period longer than 36 months. As regards the anonymisation of personal data, the organisation admits that 25% of accounts were kept for more than 36 months after the last order, formality or invoice, without being anonymised. It also admits the delay in automating the anonymisation, but disputes that there was no anonymisation of accounts.
24. **Firstly**, the Restricted Committee notes that the purpose relating to collection operations, cited by the organisation, and the related retention period could in theory only concern the data of subscribers and not of members, the latter paying immediately in exchange for receiving a document. Moreover, the Restricted Committee noted that, for this purpose as for the accounting and tax purposes, the organisation had not identified these purposes and the corresponding periods of time in its Confidentiality Charter at the time of the audit. In any event, the Restricted Committee notes that while the retention of certain data for these purposes may appear justified, it requires different actions to be taken. As such, the Restricted Committee recalls that once the purpose of the processing has been achieved, the retention of certain data for compliance with legal obligations or for pre-litigation or litigation purposes is possible, but the data must then be placed in intermediate storage, for a period not exceeding that necessary for the purposes for which they are retained, in accordance with the provisions in force. Only relevant data should be placed in interim storage, either in a dedicated archive database or by making a logical separation within the active database, allowing only authorised persons to access it. The Restricted Committee notes that on the day of the audit, none of these actions had been implemented by the organisation.
25. **Secondly**, the Restricted Committee notes that the manual anonymisation implemented by the organisation at users’ request only concerned a very small number of accounts, since on the day of the online audit, 25% of the accounts had not been anonymised even though they should have been. The Restricted Committee notes that no automatic anonymisation procedure was in

place at the time of the online audit, with the organisation retaining identifying data for an unlimited period of time in the absence of an anonymisation request from users.

26. Therefore, the Restricted Committee considers that the above facts constitute a structural breach of article 5, paragraph 1, e) of the GDPR.
27. The Restricted Committee notes that the organisation had indicated during the procedure that a purge of accounts that had been inactive for more than 36 months had been implemented since the audit, but notes that the breach was still evident with respect to the past.

B. Breaches of the obligation to ensure the security of personal data (article 32 of the GDPR).

28. Article 32 of the GDPR states that “*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.”
29. The rapporteur notes, firstly, that the delegation found that the passwords used by users to log in to their accounts, which can be accessed from the organisation’s website, are not sufficiently robust in that they are limited to eight characters, without any complexity criteria, and are not associated with any additional security measures. Furthermore, the rapporteur notes that on the day of the findings, it was impossible for all users or subscribers of the website “[REDACTED]”, i.e. for more than 3.7 million accounts, to enter a secure password because of the limitation of their size to a maximum of 8 characters.
30. Secondly, the rapporteur notes that the organisation sends non-temporary passwords for accessing accounts in clear text via email.
31. Thirdly, the rapporteur points out that the organisation also keeps passwords and secret questions and answers used during the password reset procedure by users in clear text in its database.
32. Lastly, the rapporteur notes that the organisation does not confirm to users that the password has been changed either. The rapporteur considers that users who are not alerted to unauthorised changes are therefore not protected against attempts to steal their account.
33. In light of these elements, the rapporteur considers that the various security measures put in place by the organisation are insufficient with respect to article 32 of the GDPR.
34. In its defence, the organisation argues that the security obligation is a best efforts obligation that must be assessed *concretely* and that its non-fulfilment must be established by a finding of

the ineffectiveness of the measures implemented, having led to unauthorised access, which is not the case in this instance. It stresses that the recommendation on passwords referred to by the rapporteur constitutes flexible law, that it is not a matter of mandatory rules, applicable from *an abstract* viewpoint, independently of any context, and whose non-compliance would, in itself, justify an administrative sanction. In addition, the organisation states that the data protection impact assessment revealed a low risk to personal data in the event of unauthorised access, since for member accounts, which represent the majority of accounts, bank data is not recorded, unlike for subscriber accounts, and an unauthorised third party will not be able to do anything other than purchase documents and send formalities instead of the account holder. Lastly, the organisation stresses that the information accessible by logging in to a user's account is essentially personal data present in the company registration certificate extracts and other documents that can be ordered, except in the case of accounts created by non-professionals whose identification and location data are not public.

35. First of all, the Restricted Committee recalls that, pursuant to article 32 of the GDPR, in order to ensure the protection of personal data, it is incumbent on the data controller to take "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*". The Restricted Committee considers that the use of a short or simple password without imposing specific categories of characters and without additional security measures can lead to attacks by unauthorised third parties, such as "brute force" or "dictionary" attacks, which consist of successively and systematically testing numerous passwords and therefore result in a compromise of the associated accounts and the personal data they contain. In this respect, it notes that the need for a strong password is recommended both by the *Agence Nationale de la Sécurité des Systèmes d'Information* (National Cybersecurity Agency of France - ANSSI) and by the Commission in its deliberation no. 2017-012 of 19 January 2017. In this case, the Restricted Committee notes that the passwords in question are limited to eight characters without any complexity criteria, and are not associated with any additional security measures. The Restricted Committee considers that the risk incurred by data subjects is real: a third party having had access to the password could not only access all of the personal data present in the data subject's account, but also view the history of their orders, download their invoices and/or change the account password and contact information without the user's knowledge.
36. Furthermore, the Restricted Committee considers that the methods of transmitting and storing passwords implemented by the organisation are not appropriate in view of the risk that the data subject would be exposed to if a third party were to capture their username and password. Indeed, the transmission, in clear text, of a password that is neither temporary nor for a single use and whose renewal is not made mandatory makes it easily and immediately usable by a third party, who would have undue access to the message containing it. The Restricted Committee recalls that a simple handling error can lead to the disclosure of personal data to unauthorised recipients and thereby breach individuals' privacy rights. Lastly, the Restricted Committee considers that a user who is not alerted in case of unauthorised modification is therefore not protected against attempts to steal their account.
37. Consequently, taking into account these risks for the protection of personal data and the privacy of individuals, the Restricted Committee considers that the measures deployed to guarantee data security in this case are insufficient.
38. Next, the Restricted Committee specifies that although deliberation no. 2017-012 of 19 January 2017, the CNIL guide on the security of personal data and the ANSSI technical note on passwords cited in the rapporteur's writings are certainly not imperative, they nevertheless set

out the basic security precautions corresponding to the state of the art. Consequently, the Restricted Committee recalls that it is considering a breach of the obligations arising from article 32 of the GDPR and not a failure to comply with the recommendations, which in any case provide relevant information for assessing the risks and the state of the art in terms of personal data security.

39. In addition to these recommendations, the Restricted Committee stresses that it has, on several occasions, adopted financial penalties where the characterisation of a breach of article 32 of the GDPR is the result of insufficient measures to ensure the security of the data processed, and not merely the result of the existence of a personal data breach. Deliberations no. SAN-2019-006 of 13 June 2019 and no. SAN-2019-007 of 18 July 2019 are aimed in particular at the insufficient robustness of passwords and their transmission to the organisation's customers by email, in clear text, after the account has been created.
40. In these circumstances, in view of the risks incurred by individuals, as recalled above, and the volume and nature of the personal data that may be contained in more than 3.7 million accounts (bank details of the subscriber accounts, last name, first name, postal and email address, landline and mobile telephone numbers, secret question and its answer of all of the accounts), the Restricted Committee considers that the organisation has failed to fulfil its obligations under article 32 of the GDPR.
41. The Restricted Committee notes that in the context of the present procedure, the organisation has taken certain measures to ensure the security of the data processed. Nevertheless, it considers that, since the implementation of its password policy in 2002 and until June 2021, the security measures put in place by the organisation did not enable it to ensure a sufficient level of security of the personal data processed and that, therefore, a failure to comply with the obligations of article 32 of the Regulation is established.

III. Regarding corrective powers and their publication

42. Under the terms of article 20(III) of the Act of 6 January 1978 amended:

“When the data controller or its data processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chair of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the restricted committee of the Authority with a view to the announcement, after adversarial proceeding, of one or more of the following measures: [...] 7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed EUR 10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover of the preceding financial year, whichever is greater. In the cases mentioned in 5 and 6 of article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same article 83.”

43. Article 83 of the GDPR further states that “*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive*”, before specifying the elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.

44. **Firstly**, with regard to the principle of imposing a fine, the organisation insists in its defence on the contractual responsibility of its data processor with regard to the instructions given to it concerning the security and anonymisation of personal data, on the prioritisation of other legal and regulatory projects in relation to its compliance with the GDPR, on its extensive cooperation with the CNIL and on the major efforts undertaken since the beginning of the audit.
45. The Restricted Committee notes that, in imposing an administrative fine, it must take into account the criteria specified in article 83 of the GDPR, such as the nature, severity and duration of the infringement, the number of people affected, the measures taken by the data controller to mitigate the damage suffered by the data subjects, the fact that the breach was committed due to negligence, the degree of cooperation with the supervisory authority and the categories of personal data concerned by the infringement.
46. The Restricted Committee considers firstly that although the organisation gave specific instructions on anonymisation and security to its data processor, it appears that it did not monitor the execution of these instructions and did not exercise satisfactory and regular control over the technical and organisational measures implemented by its data processor to ensure compliance with the GDPR and, in particular, to ensure the anonymisation and security of the personal data processed.
47. The Restricted Committee also considers that it is necessary to take into account the nature of the actor concerned, [REDACTED]
In this respect, the Restricted Committee considers that the organisation should therefore have been particularly rigorous in complying with all of its legal and regulatory obligations. However, it appears from the debates that the organisation has postponed the implementation of the anonymisation and security of personal data projects in order to meet other compliance obligations not related to data protection, without increasing its available resources.
48. The Restricted Committee then notes that the breaches complained of were breaches of key principles of the GDPR that were not introduced by this text but pre-existed in the “French Data Protection Act”. The Restricted Committee also emphasises that these breaches cannot be considered an isolated incident. With regard to the failure to comply with the retention period, the Restricted Committee recalls that the organisation had itself set a retention period for personal data that it had not complied with and that this breach concerns more than one million user accounts, both members and subscribers. With regard to the data security breach, the Restricted Committee considers that the extreme weakness of the password complexity rules, as well as the security measures concerning the communication, storage and renewal of passwords, in force since 2002, rendered all of the accounts vulnerable.
49. Lastly, the Restricted Committee notes that the compliance measures put in place following the notification of the sanction report do not concern all of the breaches and do not exonerate the company from its responsibility for the breaches observed.
50. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the demonstrated breaches of articles 5, paragraph 1, e) and 32 of the GDPR.

51. **Secondly**, with regard to the amount of the fine, the organisation insists in its defence on the isolated nature of the complaint that gave rise to the audit and the absence of financial gain from the breaches.
52. The Restricted Committee notes that administrative fines must be both dissuasive and proportionate. It considers that the origin of the audit, which was carried out following a single complaint, does not minimise the severity of the breaches, which in any case proved to be structural. In the present case, the Restricted Committee notes, with regard to the breach concerning the personal data retention period, that the organisation has demonstrated serious negligence concerning a fundamental principle of the GDPR and that this breach concerns more than 25% of the accounts. With regard to the security breach, the Restricted Committee notes that given the accumulation of security deficiencies, the facts observed were particularly serious, especially as they rendered all of the accounts vulnerable. The Restricted Committee then recalls that the organisation had postponed compliance with the GDPR in favour of other legal and regulatory priorities. Lastly, the Restricted Committee takes into account the organisation's activity and its financial position. It also acknowledges the efforts made by the organisation to comply throughout this procedure.
53. In view of these elements, the Restricted Committee considers that the imposition of an administrative fine of €250,000 appears justified.
54. **Lastly**, with regard to the publicity of the penalty, the organisation maintains that such a measure would be disproportionate given the harm it would cause.
55. The Restricted Committee considers that the publicity of the sanction is justified in view of the severity of the breaches noted, the nature of the actor concerned which, given its size and activity, has the human, financial and technical resources to ensure a satisfactory level of protection of personal data and the strong reputation that the website enjoys with regard to commercial data.

FOR THESE REASONS

CNIL's Restricted Committee, after having deliberated, has decided to:

- **impose an administrative fine on the Economic Interest Group [REDACTED] in the amount of 250,000 (two hundred and fifty thousand) euros for the breaches of articles 5, paragraph 1, e) and 32 of the GDPR;**
- **make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the organisation at the end of a period of two years following its publication.**

The Chair

Alexandre Linden

This decision may be appealed before the State Council within two months of its notification.

Summary Final Decision Art 60

Complaint

Administrative fine

EDPBI:FR:OSS:D:2023:475

Background information

Date of complaint:	12 December 2020
Draft decision:	19 July 2022
Revised draft decision:	N/A
Date of final decision:	08 September 2022
Processor:	N/A
LSA:	FR
CSAs:	All SAs
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 32 (Security of processing)
Decision:	Administrative fine
Key words:	Password, Data retention, Data security, Anonymisation, User account

Summary of the Decision

Origin of the case

On 12 December 2020, the LSA received a complaint concerning a website operated by the controller, which allows its users to get specific legal information on companies and/or to order certain types of documents. The complainant claimed that the controller's website stored users' passwords in clear text and that it was able to obtain its own password over the telephone by simply giving its name to the helpline operator. Following this complaint, the LSA launched an investigation to verify the compliance with the GDPR of any processing accessible from that domain, or concerning personal data collected from the latter.

Findings

During its investigation the LSA found that the controller retained the personal data of 946,023 members and 17,558 subscribers whose last order, formality or invoice was dated of more than 36 months ago, contrary to the retention period indicated in the controller's confidentiality charter. In

addition, the LSA found that no procedure for automatic deletion of these data was put in place by the controller. In its defence, the controller argued that although its confidentiality charter indicates a retention period of 36 months, it would be justified for some data to be kept for a longer period and pointed out that only about 25% of the accounts were kept for more than 36 months without being anonymised.

In this respect, while the LSA acknowledged that the retention of certain data for compliance with legal obligations or for pre-litigation or litigation purposes is possible, it noted however that the controller had not identified these purposes in its confidentiality charter, and that the retention of such data for these purposes could not in theory concern members who pay immediately in exchange for the receipt of a certain type of document. In addition, the LSA recalled that the data kept for these purposes must be placed in intermediate storage, for a period not exceeding that necessary for the purposes for which they are retained. Finally, the LSA pointed out that these data should be placed in interim storage, either in a dedicated archive database or by making a logical separation within the active database, allowing only authorised persons to access it. However, the LSA noted that none of these actions had been implemented by the controller on the day of the audit. Secondly, the LSA noted that only manual anonymisation was implemented by the controller for the deletion of accounts whose deletion was specifically requested by the users and that no automatic anonymisation procedure was in place for the other accounts. The LSA therefore concluded that the controller breached its obligation to store data for a period proportionate to the purpose of the processing pursuant to **Article 5 (1)(e) GDPR**.

Furthermore, the LSA found that the methods of transmitting and storing passwords implemented by the controller were not appropriate in view of the risk that the data subjects would be exposed to if a third party were to capture their username and password. In particular, the LSA observed that the criteria imposed by the controller for the creation of passwords to log in to the controller's website were not sufficiently robust, as they are limited to eight characters, without any complexity criteria, and are not associated with any additional security measures. The LSA also found that the controller sent non-temporary passwords for accessing accounts in clear text via e-mail. Finally, the LSA noted that the controller kept passwords, secret questions and answers used by users in clear text and did not notify them of a (possibly unauthorised) change of these passwords. In view of the risks incurred by the data subjects and the volume and nature of personal data that may be contained in more than 3.7 million accounts (including, *inter alia*, bank details of the subscriber accounts, last name, first name, postal and email address, landline and mobile telephone numbers, secret question and its answer of all of the accounts), the LSA considered that the controller failed to fulfil its obligations under **Article 32 GDPR**.

Decision

The LSA found that an administrative fine of €250,000 would be dissuasive, proportionate and justified in the case at stake. Additionally, the LSA decided to make its decision public, identifying the company by name, for a period of two years.



GZ: 2022-0.820.551

Data protection complaint (access and information)
[REDACTED]

Decision of the Data Protection Authority

CONTACT

PROVERB

The data protection authority decides on the data protection complaint of the [REDACTED] (complainant) of 19 March 2019 against [REDACTED] (respondent) for breach of the right to information and access as follows:

- The complaint will be rejected in respect of those parts relating to the partial (subsequently) fulfilled data access request as well as the right to information.

Legal bases: § 24(1) and (5) of the Data Protection Act (DSG), BGBl. I No 165/1999 as amended; Articles 13, 15, 60(9) and 77 of Regulation (EU) 2016/679 (General Data Protection Regulation — GDPR), OJ L 119, 4.5.2016, p. 1.

JUSTIFICATION

A. Arguments of the parties and proceedings

1. By complaint of 19 March 2019, improved by submissions of 2 April 2019, 23 April 2019 and 8 May 2019, the complainant claimed an infringement of the right to information and information and claimed that he had acquired a [REDACTED] a person with four training sessions per week from the Respondent in April 2018; consists of, among other things, a licensed software. By e-mail from 18 April 2018 the Complainant the

Respondent informed that medical data would be collected during the operation of the software and a monthly Data matching with the information in the Online database the The respondent seems to be taking place. The complainant then agreed with the respondent to purchase an offline variant. On 11 June 2018, the complainant received the following notification from the programme: No synchronisation has been performed for 30 days. *The program cannot be reused until a synchronisation has been carried out with an existing internet connection.*' The complainant then connected the device to the Internet. As a result, 55 entries for various training sessions were sent to the Respondent. On 7 September 2018, another synchronisation took place, in which 114 entries were transferred. The complainant was not informed by the respondent of the purposes of the data processing nor of the legal basis for this. Furthermore, the complainant had requested the respondent by e-mail of 11 September 2018 to provide information pursuant to Article 15 of the GDPR, but this request for information had not yet been answered.

2. As this is a cross-border situation and the main establishment or sole establishment of the respondent is located in Germany, the proceedings were suspended by decision of the Data Protection Authority of 21 June 2019, GZ DSB-D130.241/0006-DSB/2019 until the decision of a lead supervisory authority or the European Data Protection Board.

3. Subsequently, the Bavarian State Office for Data Protection Supervision (BayLDA) has declared itself the lead supervisory authority and submitted the Respondent's complaint for comments and made several requests in this regard.

From the respondent's point of view, the facts are different from those stated by the complainant in the following points: The purchase of the offline variant was made after consultation by the Respondent about the differences between online and offline variants. In this context, the complainant confirmed to the respondent that he waived the online synchronisation of his data. He also noted that his data could not be recovered even in the event of a loss or defect of a device. A corresponding confirmation signed by the complainant on 23 April 2018 was submitted by the Respondent. In order to be able to use the licensed offline version, an activation must be made. In this case, license data (name, address, PIN) would be requested, which the complainant had also agreed to after corresponding oral information by the

respondent. In that regard, the respondent submitted the judgment of the Amtsgericht Nürnberg of 25 March 2019 (ref. 12 C 8459/18) in which that facts were found. However, the complainant subsequently attempted to perform an online synchronisation despite the confirmation signed on 23 April 2018 and entered data. By e-mail of 12 June 2018, the Respondent agreed to the complainant to provide and activate a so-called single version. This is a software extension that allowed the complainant to train on a larger scale. The nature of the software acquired by the complainant as an offline variant was not thereby altered. However, the complainant subsequently attempted to carry out an online synchronisation and entered data contrary to the agreement reached on 23 April 2018. The message "*No synchronisation has been performed for 30 days. The program can only be reused once a synchronisation has been performed on an existing Internet connection*" is based on the fact that the complainant unlawfully installed an older software version on another device that had a software error. Therefore, instead of contacting the Respondent, the complainant carried out the synchronisation. The complainant was unable to provide proof of when and by which device this notification was displayed. Moreover, that was also stated in the above-mentioned judgment of the Amtsgericht Nürnberg. The complainant's request for information had already been answered by e-mail of 12 September 2018. A corresponding e-mail has been submitted. Neither the right to information nor the right to information have been violated.

4. By final notification of 25 November 2020, the BayLDA informed the complainant of the results of the investigation.

5. By letter dated 9 June 2021, the BayLDA requested further information from the Respondent, namely the sending of the second information provided on 13 September 2018, as well as information on the state of play of the court proceedings conducted between the complainant and the respondent. The respondent informed the BayLDA by e-mail of 3 August 2021 that the appeal against the judgment of the Amtsgericht Nürnberg of 25 March 2019 had been withdrawn. Furthermore, the information provided by e-mail of 13 September 2018 was sent.

6. With regard to the decision taken by the lead supervisory authority, the decision of the data protection authority suspending the proceedings was remedied by a decision of today's day and is issued by ggstl regarding the part of the complaint to be dismissed. Let's go.

B. Subject of complaint

The subject matter of the complaint is whether the Respondent has thereby infringed the complainant's rights of access and information by not providing him with information or sufficient information. For the part to be granted, the lead supervisory authority, the BayLDA, already has Article 60. Paragraph 9 of the GDPR. In accordance with Article 60(9) of the GDPR, the Austrian data protection authority has to decide on the parts of the complaint to be rejected, which define the subject-matter of the complaint.

C. Factual findings

The respondent has its office in Nuremberg, Germany. The complainant is domiciled in Austria.

A dispute was pending between the parties concerning the withdrawal of the complainant's contract from a [REDACTED] complete set purchased from the respondent, including a license of a so-called [REDACTED] software for training purposes, and the complainant's action in this regard — which had cited as grounds for rescission of data protection defects — was dismissed by judgment of the Amtsgericht Nürnberg of 25 March 2019 (ref. 12 C 8459/18) after conducting an oral hearing — now final.

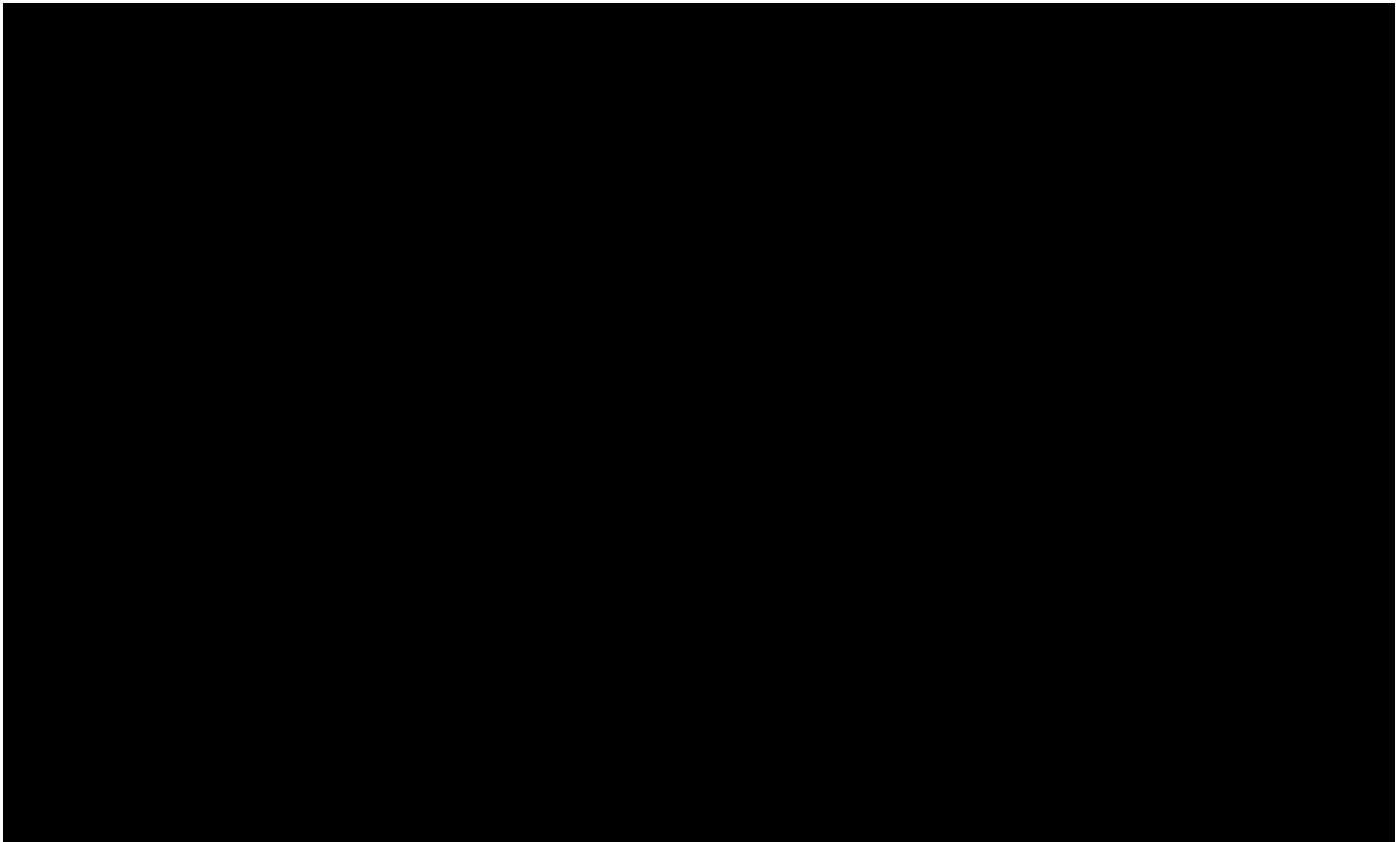
Among other things, the District Court found that the complainant initially ordered and delivered an offline version in April 2018. In June 2018, the offline version was converted into a single version at the complainant's request. Names, address and PIN number were unlocked for initial setup or licensing verification. Furthermore, the respondent's body size, weight and e-mail address were recorded. No further data query by the Respondent took place.

The complainant was informed about the licence query or now has the information concerning him or her of the respondent's data processing.

Assessment of evidence: *The findings are based first on the arguments put forward by the parties to the proceedings and from the documents in the file. As regards the information of the complainant by the respondent, in particular the judgment of the Amtsgericht Nürnberg of 25 March 2019*

(Ref. 12 C 8459/18) and the BayLDA's final communication of 25 November 2020.

On the basis of the complainant's request of 11 September 2018, the Respondent provided the following information by letters of 12 September and 13 September 2018:



In addition, except for the clear data processed by the Respondent, which have been unsolicited by the Respondent, the Complainant has been informed of his data processed by the Respondent.

Assessment of evidence: The finding is based, in particular, on the judgment of the Amtsgericht Nürnberg of 25 March 2019 (ref. 12 C 8459/18) as well as on the final notification of the BayLDA of 25 November 2020 and the contents of the file.

By complaint of 19 March 2019, the complainant brought a data protection complaint to the Austrian data protection authority for breach of the right to information and information.

Assessment of evidence: The finding is based on the arguments put forward by the parties and the content of the file.

D. From a legal point of view, it follows:

The complaint processing is a cross-border data processing within the meaning of Article 4(23)(b) of the GDPR, since the complainant is domiciled in Austria, but the controller (respondent) is established in Nuremberg, Germany. In accordance with Article 56(1) GDPR, the lead supervisory authority was therefore

the Bavarian State Office for Data Protection Supervision (BayLDA). According to Art. 4 para. 22 lit. c GDPR, the Austrian data protection authority was the supervisory authority with which the complaint was submitted.

In the course of the proceedings, the lead supervisory authority concluded that the respondent infringed the complainant's right of access by providing data information but not providing clear information to the complainant. In this regard, the BayLDA referred to Guidelines 01/2022 on data subject rights — Right of access, EDPB, para. 19 (version 1.0, adopted on 18 January 2022) and on ErwGr. 63 of the GDPR.

Furthermore, the BayLDA considered that the deletion of the complainant's data after the court hearing before the Amtsgericht Nürnberg resulted in an infringement of the complainant's right to information, since the complainant did not request such deletion and therefore it became impossible to inform the complainant's clear data. In this respect, the BayLDA again referred to the Guidelines 01/2022, specifically para. 39.

Moreover, the BayLDA considered that the right to information was not infringed. Also the alleged infringement in the right to information iSd. Article 13 of the GDPR considered the BayLDA not infringed on the basis of the findings of the investigation. Nor could it be contradicted.

The judgment of the Amtsgericht Nürnberg of 25 March 2019 (ref. 12 C 8459/18) already shows that the respondent has complied with its obligation to provide information and is also apparent from the findings that the complainant now has the information in accordance with Article 13(4) of the GDPR. A right to a declaration that the information has been given too late cannot be derived from the GDPR (see, for this purpose, the judgment of the Verwaltungsgerichtshof of 27 September 2007, with regard to the comparable legal situation under the DSG 2000. 2006/06/0330, mwN). In any event, the success of a complaint pursuant to Article 77(1) of the GDPR in conjunction with Paragraph 24(1) of the DSG is conditional on the existence of a specific complaint at the time of the administrative decision, which is no longer apparent at the time of the administrative decision (see, for example, VwSlg 11.568 A/1984 mwN regarding the lack of a subjective infringement).

This also applies to the other points to be reported iSd. Art. 15 GDPR, of which the complainant (in the meantime) is aware (e.g. the possibility of lodging a complaint with a supervisory authority or the purposes of processing; see the findings of the VwGH of 27 March 2006, ZI. 2004/06/0125, of 25 April 2006, ZI. 2004/06/0167, and of 25 November 2008, ZI. 2004/06/0007).

If the lead supervisory authority and the supervisory authorities concerned agree to reject or accept parts of the complaint and to act on other parts of that complaint, Article 60 shall apply. Paragraph 9 GDPR on this matter makes a separate decision for each of these parts. The lead supervisory authority shall adopt the decision for the part concerning action in relation to the controller, notify it to the principal establishment or

sole establishment of the controller or processor in the territory of its Member State and inform the complainant thereof, while the supervisory authority responsible for the complainant adopts the decision for the part concerning the rejection or rejection of that complaint and informs the complainant and informs the controller or processor thereof. For this reason, the decision in question is taken by the Austrian Data Protection Authority for the part of the complaint to be dismissed.

The appeal was therefore dismissed in accordance with the opposition.

NOTICE OF APPEAL

A complaint may be lodged in writing to the Federal Administrative Court against this decision within four weeks of notification. The complaint must **be submitted to the Data Protection Authority** and must:

- the name of the contested decision (GZ, subject)
- the name of the competent authority;
- the reasons on which the claim of illegality is based;
- the desire and
- contain the information necessary to assess whether the complaint is submitted in good time.

The data protection authority has the possibility to amend its **decision within two months either by means of** a preliminary appeal decision or to **submit the complaint to the Federal Administrative Court with the file of the** proceedings.

The complaint against this decision is subject to **a fee**. The fixed fee for a corresponding entry including supplements is **EUR 30**. The fee is paid to the tax office's account for fees, traffic taxes and gambling (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW) to be paid, whereby the respective complaint procedure (business number of the decision) must be indicated on the payment order as the intended use.

In the case of electronic transfer of the appeal fee with the "Finance Office payment", the tax office for fees, traffic taxes and gambling (IBAN as before) must be indicated or selected as the recipient. Furthermore, the tax number/tax account number 109999102, the tax type 'EEE complaint fee', the date of the decision as the period and the amount must be indicated.

The payment **of the fee** must be **proved** in original (original) upon lodging **the complaint to the Data Protection Authority** by means of a proof of payment confirmed by a post office or a credit institution confirming the entry. If the fee is not paid or not paid in full, a **report will be sent to the responsible tax office**.

A timely and admissible complaint to the Federal Administrative Court **shall have suspensive effect**. The suspensory effect may have been excluded in the judgment or may be ruled out by a decision of its

own.

January 9, 2023

GZ: D155.026
2022-0.029.027

Barichgasse 40-42
A-1030 Vienna
Tel.: + 43-1-52152 [REDACTED]

E-mail: dsb@dsb.gv.at

Desk officer: [REDACTED]

[MACHINE TRANSLATION]

Please note that this decision only revolves around a formal infringement of the processing that took place in August 2020. According to our Austrian Data Protection Act, we have the obligation to formally establish such infringements, if requested by the complainant. We did not exercise our corrective powers because the tool was removed from the website at stake before the conclusion of this case.

Data protection complaint (Art. 77 para. 1 GDPR)

[REDACTED], represented by NOYB/1. [REDACTED] and 2.

Google LLC by e-delivery/email "email address"

DECISION

The Austrian Data Protection Authority decides on the data protection complaint of [REDACTED] (complainant) of 18 August 2020, represented by NOYB — European Centre for Digital Rights, Goldschlagstraße 172/4/3/2, 1140 Vienna, ZVR: 1354838270, against 1) [REDACTED] [REDACTED] (first respondent), represented by [REDACTED] [REDACTED] and 2) Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (second respondent), represented by [REDACTED]

[REDACTED], for breach of the general principles of

Data transfer pursuant to Art. 44 GDPR as follows:

1. The decision of the Data Protection Authority of 2 October 2020, Zl. D155.026, 2020-0.526.838, is removed.
2. The complaint against the first respondent is justified and it is established that:

- a) the first respondent as responsible by implementing the tool “Google Analytics” on its website at www.█████.at has transmitted personal data of the complainant to the second respondent at least on 11 August 2020 (these are at least unique user identification numbers, IP address and browser parameters);
 - b) the standard data protection clauses adopted by the first respondent with the Second respondent has not provided an adequate level of protection in accordance with Article 44 of the GDPR, since
 - i) the Second respondent as Supplier electronic Communication services within the meaning of 50 U.S. Code § 1881(b)(4) is qualified and as such is subject to surveillance by U.S. intelligence services pursuant to 50 U.S. Code § 1881a (“FISA 702”), and
 - ii) the measures taken in addition to those referred to in point 2(b)
Standard data protection clauses are not effective as they do not eliminate the monitoring and access possibilities of US intelligence services;
 - c) in the present case, no other instrument under Chapter V of the GDPR for the transfer of data referred to in point 2.a) can be used and the first respondent has therefore not ensured an adequate level of protection in accordance with Article 44 of the GDPR for the data transfer referred to in point 2.a).
3. The complaint against the second respondent for an infringement of the general principles of data transfer pursuant to Article 44 GDPR is dismissed.

Legal bases: Articles 4(1), 2, 7, 8 and 23(b), Article 5, Article 44, Article 46(1) and (2)(c), Article 51(1), Article 56(1), Article 57(1)(d) and (f), Article 60(7) and (8), Article 77(1), Article 80(1) and Article 93(2) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), OJ L 119, 4.5.2016 p. 1; Sections 18(1) and 24(1), (2)(5) and (5) of the Data Protection Act (DSG), BGBI. I No 165/1999 as amended; Section 68(2) of the General Administrative Procedures Act 1991 (AVG), BGBI. 51/1991, as amended.

REASONS FOR THE DECISION

A. Arguments of the parties and procedure

A.1. In its submission of 18 August 2020, the complainant submitted the following summary:

On 11 August 2020, at 1:46:00, he visited the first respondent’s website at www.█████.at. During the visit, he was logged into his Google account, which was linked to the complainant’s e-mail address. The first respondent embedded an HTML code for Google services (including Google Analytics) on its

website. During the visit, the first respondent processed personal data, namely at least the complainant's IP address and cookie data. Some of these data were transmitted to the second respondent. Such a transfer of data requires a legal basis in accordance with Art. 44 et seq. of the GDPR.

According to the judgment of the Court of Justice of 16 July 2020, Case C-11/18 ('Schrems II'), the respondents could no longer rely on an adequacy decision ('Privacy Shield') pursuant to Article 45 GDPR for data transfer to the USA. The first respondent should also not base the transfer of data on standard data protection clauses where, in accordance with Union law, the third country of destination does not ensure adequate protection of personal data transmitted on the basis of standard data protection clauses. The second respondent must be classified as a provider of electronic communications services within the meaning of 50 U.S. Code § 1881(b)(4) and, as such, is subject to supervision by US intelligence services under 50 U.S. Code § 1881a ("FISA 702"). The second respondent actively provides personal data to the U.S. Government pursuant to 50 U.S. Code § 1881a.

Consequently, the respondents are not in a position to ensure adequate protection of the complainant's personal data when his data are transferred to the second respondent. The transfer of the complainant's data to the USA was unlawful. The complaint was accompanied by several annexes.

A.2. With opinion of 22. December 2020, the First respondent
summarising the following:

The program code for the Google Analytics tool was embedded on www.█████.at. Without consent, however, the code would not be played by the web server. The first respondent is established only in Austria and has no other branches in other Member States. It operates the following European versions of the website, on which the tool is also integrated in the same form: www.█████.at, www.█████.de, www.█████.eu, www.█████.co.uk and ♦.

The tool would be used to enable general statistical analyses of the behaviour of the website visitors. However, the tool does not allow the content or search queries to be adapted to a specific website user, since the evaluation is carried out anonymously and does not allow any connection to a particular user. User IP addresses would also be anonymised prior to storage or transmission ("IP anonymisation"). The function "anonymizeIP" was set to "true". This ensures anonymisation before storing the data. The code for the tool in question is currently still available on the websites.

If the GDPR is applicable, the first respondent is the controller and the second respondent is a processor. A processor agreement was concluded. As no personal data would be transferred, the judgment of the CJEU of 16 July 2020 in Case C311/18 is not relevant. However, in order to make arrangements for the possible transfer of personal data to the second respondent — e.g. in the event that IP anonymisation is deactivated on the basis of a data breach — the first respondent concluded a processor agreement with the second respondent, as well as standard data protection clauses (SDK). This was implemented purely for precautionary reasons. The second respondent put in place further technical and

organisational measures to provide a high level of data protection for the data processed through the tools. The opinion was accompanied by a number of annexes.

A.3. In a summary of comments of 12 February 2021, the complainant submitted the following:

The first processed IP address would — if at all — be anonymised later in a second step. This possible anonymisation after transfer does not affect the previous processing. The opinion contains a detailed technical description here. If the first respondent is convinced that no personal data will be processed, for example, the conclusion of order processing conditions is absurd. The opinion was accompanied by a number of annexes. It is requested to establish that the data transfers in question were inadmissible within the meaning of Article 44 et seq. of the GDPR.

A.4. The DPA requested the second respondent, with discharge of 3 May 2021, as follows (formatting not reproduced 1:1):

"Concerns: I. Data protection complaint pursuant to Art. 77 para. 1 GDPR against Google LLC; II. To the questionnaire of 9 April 2021

I. Data protection complaint pursuant to Art. 77 para. 1 GDPR against Google LLC

In the annex you will find a data protection complaint dated 18 August 2020 pursuant to Art. 77 para. 1 GDPR of MB (complainant), represented by NOYB, an organisation pursuant to Art. 80 (1) GDPR, against 1. [REDACTED] (first respondent) and 2. Google LLC (second respondent). In addition, the first respondent's observations of 16 April 2006 will be submitted. Submitted in December 2020.

Subject of appeal is the use of the Google Analytics tool by the first respondent on his website. Google LLC is expressly mentioned as a second respondent. A violation of the requirements for international data traffic (Chapter 5 GDPR) is alleged.

You will be given the opportunity to comment on this complaint within a period of three weeks from the date of receipt of this letter.

II. To the questionnaire of 9 April 2021

Google LLC has already completed a questionnaire from the Data Protection Authority on Google Analytics in parallel pending complaints on the number of transactions DSB-D155.027 and submitted corresponding replies to the Data Protection Authority by letter dated 9 April 2021.

It is noted that Google's opinion of 9 April 2021 is formulated in such a way that the explanations are also applicable to the relevant appeal proceedings against the price comparison of [REDACTED]. Consequently, the Data Protection Authority intends to grant the parties involved in the present proceedings parties to the letter of 9 April 2021 from Google LLC.

If you have any objections to this procedure, you will be asked to notify it within three weeks of receipt of this letter.

Please indicate the business number DSB-D155.026 when submitting your submissions to the data protection authority."

A.5. In its observations of 28 May 2021, the first respondent submitted, in summary, the following:

The code at issue for the Google Analytics tool was removed on 25 May 2021. The use of Google Analytics on the website www.█████.at was discontinued. A procedure under Paragraph 24(6) of the DSG (formless attitude) was suggested.

A.6. In a summary of comments of 8 June 2021, the complainant submitted the following:

It is a matter of fact which is in the past and the removal of the program code does not alter the complainant's complaint. The data in question had already been transmitted in violation of Article 44 et seq. of the GDPR. Such a finding was requested.

A.7. By discharge of 25 June 2021, the DPA transmitted to the complainant and to the first respondent the aforementioned observations of the second respondent of 9 April 2021.

A.8. In its observations of 6 August 2021, the first respondent submitted, in summary, the following:

She used the free version of Google Analytics. In doing so, it agreed to the terms of use as well as to the SCC. The data exchange setting was not activated. Google Signals were not used either. In connection with the use of Google Analytics, it was not based on the exception provided for in Article 49(1) GDPR.

A.9. In a summary of comments of 13 August 2021, the complainant submitted the following:

Reference was made to the opinion of 5 May 2021 on the parallel procedure with the JCC: DSB-D155.027. As in the parallel proceedings, the transmitted HAR file could be used to detect that personal data of the complainant had been processed and that the data was transferred to the USA to Google LLC.

A.10. In its observations of 23 August 2021, the first respondent submitted, in summary, the following:

The first respondent is the operator of the █████ settlement portal. She operates █████ in the following language versions: █████.de, █████.eu, █████.co.uk and █████.pl.

A.11. In its observations of 2 November 2021, the second respondent submitted, in summary, the following:

The IP address at issue and the cookie data are not personal data. The IP anonymisation function was

activated. Nor is the data attributable to the complainant. The complainant did not explain which IP-address used the Internet-connected device with which he visited the website. It is also unclear whether it was a dynamic or static IP address.

However, even assuming that personal data are available, a risk-based approach should be taken when assessing the adequacy of the transfer to the US. This should be derived from the EDPB's "Schrems II" FAQ and from the European Commission's decision of 4 June 2021 on the new standard contractual clauses. In the present case, account must be taken of the fact that the transmission of the data at issue in the proceedings entails — if at all — only a low basic risk. There is also no disclosure in accordance with PO 12.333, as the aforementioned provision does not authorise the U.S. government to enforce or even request user data from a US provider, it does not receive any instructions addressed to service providers outside the U.S.. FISA § 702 is also irrelevant in view of the encryption and anonymisation of IP addresses. The second respondent concluded standard contractual clauses with the first respondent. In addition, he implemented additional measures to supplement the standard contractual clauses.

Finally, it should be noted that an infringement of Article 44 et seq. of the GDPR cannot be invoked in the context of a data protection complaint. Nor does the DPA have any competence to identify infringements in the past. In addition, Article 44 et seq. of the GDPR applies only to data exporters.

A.9. With comments of 3. In summary, the complainant submitted the following comments on December 2021:

There is a processing of personal data, evidenced by, inter alia, the annexes submitted. For the account configuration in the Google account one already had in parallel proceedings with the GZ: DSB-D155.027 delivered an opinion.

The IP anonymisation in question takes place only after the transfer to the sphere of Google LLC. Moreover, the fact that it is made within the EEA is a mere assertion which the first respondent must prove as an accountable controller. Moreover, the fact that personal data actually leave the EEA geographically is not decisive for an access by US authorities. 50 U.S. Code § 1881a ("FISA 702") is not limited to data processed geographically in the USA, but claims global validity.

In addition, it should be noted that the combination of cookie data and IP addresses in particular could be linked to tracking and the analysis of geographical location, internet connection and context of the visitor with the cookie data already described. The GDPR also has no "risk-based approach" in Chapter V. This can only be found in certain articles of the GDPR, such as Article 32 leg.cit.

Even if the second respondent did not infringe Article 44 et seq. of the GDPR, the provisions pursuant to Article 28(3)(a) and Article 29 of the GDPR must be taken into account as a 'temporary provision'. If the second respondent follows a corresponding instruction from a US intelligence service, he thus makes the decision to process personal data beyond the specific mandate of the first respondent pursuant to

Articles 28 and 29 of the GDPR and the corresponding contractual documents. As a result, the second respondent becomes the person responsible in accordance with Article 28(10) GDPR. Consequently, the second respondent must, in particular, also comply with the provisions of Article 5 et seq. of the GDPR. A secret transfer of data to US intelligence services in accordance with the law of the United States is without doubt incompatible with Art. 5 para. 1 lit. f GDPR, Art. 5 para. 1 lit. a GDPR and Art. 6 GDPR.

A.10. With opinion of 21. December 2021 brought by the first respondent summarising the following:

As already stated, it did not use Google Signals. As a technically used service provider, the second respondent expressly stated in its comments of 2 November 2021 that IP anonymisation takes place in principle only within the EEA. Only in exceptional cases would web servers outside the EEA be used. In the present case, normal operating conditions would be in place.

A.11. By observations of 9 February 2022, the second respondent essentially reiterated the previous arguments.

It was also argued that the position taken by the complainant had particularly serious and far-reaching practical consequences. This position would cause serious damage to both Austrian companies operating on the world market and the pan-European economy. The web browser-related data at issue are not sufficiently specific to ‘separate’ a browser. U.S. intelligence services have never issued an order under FISA 702 as regards the type of Google Analytics data at issue.

It is inadmissible to accept the application of a reversal of the burden of proof to the question of the personal reference of the data. The GDPR has no such reversal of the burden of proof. Moreover, this is incompatible with the principles of Austrian procedural law and the presumption of innocence.

Furthermore, there is no representative standing under Article 80(2) GDPR in Austria and cannot be circumvented by allowing NOYB to be mandated by one of its employees for the purpose of conducting a ‘model procedure’.

The opinion was accompanied by two documents.

A.9. In its last opinion of 1 March 2022, the complainant essentially reiterated the previous submissions.

B. Subject matter of the complaint

On the basis of the complainant’s submissions, it is clear that the subject-matter of the appeal is whether the first respondent has ensured an adequate level of protection in accordance with Article 44 of the GDPR for the transfer of the complainant’s personal data to the second respondent, which was <http://www.████████.at> triggered by the implementation of the Google Analytics tool on its

website www.█████.at.

For example, in its observations of 11 February 2021 and 8 June 2021, the complainant expressly requested, pursuant to Section 24(2)(5) of the DSG, that the data transfers in question were inadmissible pursuant to Article 44 of the GDPR.

In this context, it is also necessary to clarify whether, in addition to the first respondent (as data exporter), the second respondent (as a data importer) was obliged to comply with Article 44 GDPR.

The request to impose an immediate ban on the first respondent (as the responsible party) on the transfer of data to the second respondent cannot be ruled out, since the latter has temporarily removed the Google Analytics tool from its website.

Finally, it should be noted that the partial notice in question does not deny the alleged infringements of the second respondent pursuant to Article 5 et seq. of Article 28(3)(a) and Article 29 of the GDPR. Further investigative steps are necessary in this respect and will be discussed in a further decision.

C. Findings of fact

C.1. In any event, the first respondent was the operator of the █████ service in August 2020. █████ is an online comparison portal where products can be compared. In this way, consumers can find the cheapest supplier for a specific product, which is listed by the first respondent.

The first respondent operates the website www.█████.at for the Austrian market <http://www.█████.at/>. In addition, the first respondent also operates █████ for the German market (www.█████.de), the English-speakingmarket (www.█████.eu), the Polishmarket (www.█████.pl) and the UK market (www.█████.co.ukwww.█████.co.uk). The first respondent is established only in Austria and has no other establishments in other Member States of the European Union.

Assessment of evidence in relation to C.1.: The findings made are based on the observations of the first respondent of 22 February 2006. December 2020 (Question 2) and was not disputed by the complainant. In addition, the findings made are based on an official search carried out by the Data Protection Authority at www.█████.at <http://www.█████.at/>(requested 18 March 2022).

C.2. The second respondent developed the tool Google Analytics. Google Analytics is a measurement service that enables customers of the second respondent to measure traffic characteristics, among other things. This includes measuring the traffic of visitors visiting a specific website. This makes it possible to understand the behaviour of website visitors and to measure how they interact with a specific website. Specifically, a website operator can create a Google Analytics account and view reports about the website using a dashboard. Google Analytics can also measure and optimise the effectiveness of advertising campaigns that website owners carry out on Google ad services.

There are two versions of Google Analytics: A free version as well as a paid version called Google Analytics 360. The second respondent made the free version available until the end of April 2021. Both versions of Google Analytics have been provided by Google Ireland Limited since the end of April 2021.

Assessment of evidence in relation to C.2.: The findings were based on the second respondent's comments of 9 April 2021 (p. 3 and questions 1 and 2) and were not contested by the complainant. The second respondent's observations of 9 April 2021 were originally conducted in parallel proceedings with the CCC: DSB-D155.027 and brought to the attention of the parties to the present proceedings, as the comments are general comments on the functioning of Google Analytics.

C.3. In any event, the first respondent — as a website operator — took the decision on 11 August 2020 to use the free version of the Google Analytics tool for its [REDACTED] websites. To this end, it has installed a JavaScript code ("tag") provided by the second respondent in the source code of its website. The first respondent used the tool to enable general statistical analyses of the behaviour of website visitors. The Google Signals add-on tool has not been activated.

In any case, these analyses are used by the first respondent to present the content of the website [www.\[REDACTED\].at](http://www.[REDACTED].at) in accordance with the general interest of the subject in such a way that the most requested channels can be put in the foreground and the presentation can be adjusted according to the topicality of a specific topic.

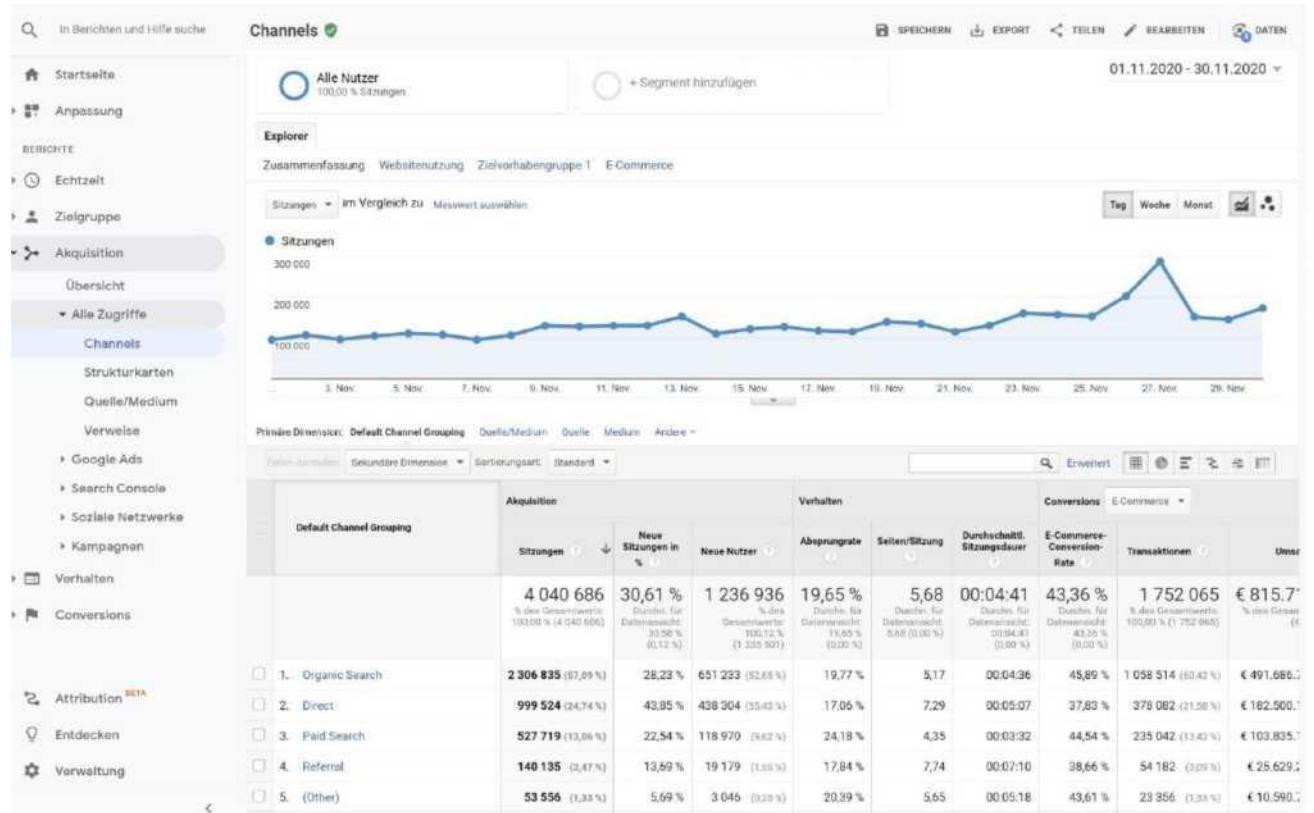
The first respondent created a Google Analytics account for this purpose. The Google Analytics account ID with the account name "[REDACTED].at" is 109732782. The above evaluations

can be carried out by the first respondent by logging into the “█████.at” Google Analytics account and in the dashboard reports on the traffic of www.█████.at. The reports are divided into real-time, target groups, acquisitions, behaviors and conversions. The first respondent can select custom requirements for reporting, the second respondent has no influence on this. Nor does the second respondent have any influence on the extent to which the first respondent subsequently uses the reports drawn up.

The dashboard is excerpt as follows (formatting not reproduced 1:1):

The screenshot shows the 'Account settings' page in Google Analytics. The left sidebar lists navigation options: ADMINISTRATION (with a search icon), USERS, Home (blue), Create an account (blue), mischievous at (dropdown), Account settings (red), 211 Account — User Validation, T All filters, Account change history, and | Recycle bin. The main content area is titled 'Account settings' with a 'Move to Papier Basket' link. It shows 'Basic settings' with 'Account ID' (█████) and 'Account name' (█████). Below that is 'Country of company' set to 'Austria *'. A section titled 'Data Sharing Settings' explains data security and includes a checkbox for 'Google products and services RECOMMENDED'. The checkbox description states: 'Share Google Analytics data for Google to help improve Google's products and services. This allows us to continuously optimise the Google Analytics service 'Analytics Radar' as well as statistics. In addition, you contribute to improving our spam detection that benefits all linked products as well as other users. If you additionally enable Google signals, you can also use advanced reports on demographic characteristics and interests. If you disable this option, data may continue to be sent to other Google products associated with your property.' A note below says: 'With Data Sharing Options, you can better control which Google Analytics data others can access [More information](#)'.

A No action required



Assessment of evidence relating to C.3: The findings made are based on the submission of the first respondent dated 22. December 2020 and were not contested by the complainant. The above screenshots have been taken from the enclosed Supplement./B and./D.

C.4. The Google Analytics tool has the following functionality: When visitors view the

website www.████████.at the JavaScript code inserted in the source code of the website refers to a JavaScript file previously downloaded to the user's device, which then executes tracking operation for Google Analytics. The tracking operation retrieves data via the page request by various means and sends this information to the analytics server via a list of parameters connected to a single pixel GIF image request.

The data collected using Google Analytics on behalf of the website operator comes from the following sources:

- the user's HTTP request;
- Browser/system information;
- (First party) Cookies.

An HTTP request for each website contains details about the browser and the computer that makes the request, such as host name, browser type, referrer and language. In addition, the DOMinterface of the browsers (the interface between HTML and dynamic JavaScript) provides access to more detailed

browser and system information, such as Java and Flash support and screen resolution. Google Analytics uses this information. Google Analytics also places and reads first-party cookies on a user's browsers that enable the measurement of user session and other information from the page request.

When all this information is collected, it is sent to the Analytics servers in the form of a long list of parameters sent to a single GIF image request (the meaning of the GIF request parameters is described here) to the domain google-analytics.com. The data contained in the GIF request are those that are sent to the analytics servers and then processed and end up in the reports of the website operator.

On the second respondent's information page on the Google Analytics tool, extracts of the following information (formatting not reproduced 1:1, requested on 18 March 2022):

gtag.js and analytics.js (Universal Analytics) — cookie usage

The [analytics.js JavaScript library](#) or the [gtag.js JavaScript library](#) can be used for [Universal Analytics](#). In both cases, the libraries use *first-party* cookies to:

- Distinguish unique users
- Throttle the request rate

When using the [recommended JavaScript snippet](#) cookies are set at the highest possible domain level. For example, if your website address is blog.example.co.uk, analytics.js and gtag.js will set the cookie domain to .example.co.uk. Setting cookies on the highest level domain possible allows measurement to occur across subdomains without any extra configuration.

★ Note: gtag.js and analytics.js do not require setting cookies to transmit data to Google Analytics.

gtag.js and analytics.js set the following cookies:

Cookie name	Default expiration time	Description
_GA	2 years	Used to distinguish users.
_gid	24 hours	Used to distinguish users.
_gat	1 minute	Used to throttle request rate. If Google Analytics is deployed via Google Tag Manager, this cookie will be named _dc_gtm_<property- id>.
AMP_TOKEN	30 seconds to 1 year	Contains a token that can be used to retrieve a Client ID from AMP Client ID Service. Other possible values indicate opt-out, inflight request or an error Retrieving a Client ID from AMP Client ID Service.
gac<Property-id>	90 days	Contains campaign related Information for the user. If you have linked your Google Analytics and Google Ads accounts, Google Ads website conversion tags will read this cookie unless you opt-out. Learn more .

Assessment of evidence for C.4.: The findings made are based on the observations of the second respondent of 9 April 2021 (Question 2) in parallel with the CV: DSB-D155.027; and one amnesia Research the Data Protection Authority under <https://developers.google.com/analytics/devguides/collection/gajs/cookie-usage> and also <https://developers.google.com/analytics/devguides/collection/gtagjs/cookies-user-id> (both queried on 18 March 2022).

C.5. The respondents have entered into a contract entitled "Conditions of Processing for Google Advertising Products". This contract was valid as of 1 January 2020 at least on 11 August 2020. The

contract regulates order processing conditions for “Google advertising products”. It applies to the provision of processor services and related technical support services to customers of the second respondent. The aforementioned contract in the version of 1 January 2020 (opinion of the respondent of 22 January 2020) December 2020, Supplement./G) is based on the factual findings. That contract was subsequently updated on 12 August 2020 and 16 August 2020.

In addition, first and second respondents have a second contract entitled "Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors". These are standard contractual clauses for international data traffic. This contract, too (opinion of the respondents of 22 February 2006). December 2020, Supplement./K) is based on the findings of fact.

In the first contract, with regard to the “Conditions of Processing for Google Advertising Products” covered Categories of data to the Link <https://privacy.google.com/businesses/adsservices/> referenced. Under the link mentioned above, extracts of the following are displayed (red emphasis by the DPA, formatting not reproduced 1:1, queried on 18 March 2022):

Order data processing conditions:

Processors' services

The following Google services fall within the scope of the order data processing conditions for Google advertising products:

- Ads Data Hub
- Audience Partner API (former name: DoubleClick Data Platform)
- Campaign Manager 360 (former name: Campaign Manager)
- Display & Video 360 (former designation: DoubleClick Bid Manager)
- Extended conversions
- [Google Ad Manager Processor Functions](#)
- [Google Ad Manager 360-processor functions](#)
- Google Ads Customer Matching
- Google Ads Retail Sales (direct upload)
- Google Analytics
- Google Analytics 360
- Google Analytics for Firebase
- Google Data Studio
- Google Optimise
- Google Optimise 360
- Google Tag Manager
- Google Tag Manager 360
- Search Ads 360 (former name: DoubleClick Search)

Google is entitled to update this list in accordance with the terms of the order data processing conditions for Google advertising products.

Types of personal data

With regard to the order data processing conditions for Google advertising products (and depending on which processor services are used under the respective agreement), the following types of personal data may constitute the customer's personal data:

Processors' services	Types of personal data
Ads Data Hub	Online markings (including cookie identifiers), Internet protocol addresses and device identifiers, from Markings awarded to customers
Audience Partner API (former name: DoubleClick Data Platform)	Online markings (including cookie identifiers) and device identifiers
Campaign Manager 360 (former name: Campaign Manager)	Online markings (including cookie identifiers), internet protocol addresses and device identifiers, precise location data, customer-assigned markings
Display & Video 360	Online markings (including cookie identifiers), internet protocol addresses and device identifiers, precise location data, customer-assigned markings
Extended conversions	Names, e-mail addresses, telephone numbers, addresses, markings provided by the customer, onlinemarkings (including Internet protocol addresses)
Google Ad Manager Processor functions	Encrypted signals
Google Ad Manager 360— Processor functions	Encrypted signals
Google Ads Customer Matching	Names, e-mail addresses, addresses and markings provided by the partner
Google Ads Retail Sales (direct upload)	Names, e-mail addresses, phone numbers and addresses
Google Analytics 360	Online markings (including cookie identifiers), Internet protocol addresses and device identifiers, from Markings awarded to customers
Google Analytics	Online markings (including cookie identifiers), Internet protocol addresses and device identifiers, from Markings awarded to customers

In addition to the conclusion of standard contractual clauses, the second respondent has implemented further contractual, organisational and technical measures. These measures complement the obligations contained in the standard contractual clauses. The measures are described in the second respondent's observations of 9 April 2021 (Question 28). This description is based on the findings of fact.

The second respondent regularly publishes so-called transparency reports on data requests from US authorities. These are available at:

<https://transparencyreport.google.com/user-data/us-national-security?hl=en>

Assessment of evidence relating to C.5.: The findings made are based on the observations of the first respondent dated 22. December 2020, question 15. The above supplements are included in the Act and are known to all parties. In addition, the findings made are based on a
amnesia Research the Data Protection Authority under
https://privacy.google.com/businesses/adsservices/ (requested 18 March 2022). The findings made with regard to the 'additional measures implemented' stem from the second respondent's observations of 9 April 2021 (question 28) and from the observations of the first respondent of 22 April 2021. December 2020 (Question 23). The second respondent's observations of 9 April 2021, which in parallel proceedings with the GZ: DSB-D155.027 is included in the present act and is known to all parties. The finding with regard to the transparency reports results from an official search carried out by the DPA under

<https://transparencyreport.google.com/user-data/us-national>

security?hl=en (requested 18 March 2022).

C.6. In the course of the use of the Google Analytics tool, the possibility to use an “IPanonymisation function” is offered. This function was used by the Respondent. As part of the embedding of Google Analytics on the website, the function “anonymizeIP” was set to “true”. However, when loading the relevant scripts of Google servers, the full IP address of a website visitor is transferred to the second respondent. The IP address will only be masked in a second step after it has been entered into the Analytics data acquisition network.

For this purpose: has: the Second respondent to of his

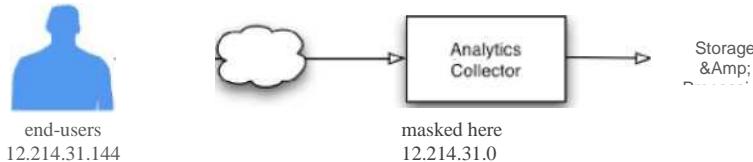
Website under

<https://support.google.com/analytics/answer/2763052?hl=de> provided the following information (excerpt, formatting not reproduced 1:1):

Detailed information

AnonymizeIP [13](#) is available in Analytics (in the library “gtag.js” is the gtag (‘con-Fig’, ‘<GA_MEASUREMENT_ID> j ('anonymize_ip': true))). This enables website owners to request that all IP addresses of their users be anonymised within the product. For example, own privacy statements or the recommendations of local data protection supervisory authorities can be implemented in some countries, which may prohibit the storage of complete IP addresses. The IPs are anonymised or masked as soon as the data is received by Google Analytics and before it is stored or processed.

IP anonymisation in analytics takes place in two steps within the data collection system: via the JavaScript tag and the data acquisition network. These steps are explained below.



Assessment of evidence relating to C.6.: The findings made are based on the observations of the first respondent of 22 February 2006. December 2020 (Question 2) and the annex./C. From Supplement./C, it is clear that the second respondent himself states that the anonymisation of the IP address takes place only in the second step after the collection of data. The finding regarding the date of anonymisation of the IP address is also based on the complainant's comments of 11 February 2021 (p. 2 f). Finally, the findings made are based on:

one amnesia Research the
Website under

<https://support.google.com/analytics/answer/2763052?hl=de> (requested 18 March 2022). As can be seen from the legal assessment, it may not be necessary to determine whether the IP address of the complainant's terminal device was masked within or outside the EEA area in the present case. Findings in this respect could therefore not be made.

C.7. The complainant visited the website www.█████.at at least on 11 August 2020. During the visit, he was logged into his Google account. A Google account is a user account used for authentication with various Google online services of the second respondent. For example, a Google account is a prerequisite for the use of services such as “Gmail” or “Google Drive” (a file hosting service).

Assessment of evidence relating to C.7.: The findings were based on the complainant's submission of

18 August 2020 (p. 2 f) and were not contested by the respondents. The findings made with regard to the basic functions of a Googleaccount are based on an official search carried out by the data protection authority at <https://support.google.com/accounts/answer/27441?hl=de> https://support.google.com/accounts/answer/27441?hl=de and <https://policies.google.com/privacy> (<https://policies.google.com/privacy> (both consulted on 18 March 2022).

C.8. In the disputed transaction between the complainant's browser and <https://████████.at/> on 11 August 2020, at 01:26:21.206 CET unique useridentification numbers were processed at least in the cookies "_ga" and "_gid". Subsequently, on 11 August 2020, at 01:26:23.795 CET, these identification numbers were sent to <https://www.google-analytics.com/collect> and thus to the second respondent.

Specifically, the following user identification numbers, which are located in the complainant's browser, were transmitted to the second respondent (same values, which each occurred in different transactions, were marked with colors:

Domain	Name	Wert	Zweck
https://████████.at/	_ga	GA1.1.165363541. 1597101359	Google Analytics
https://████████.at/	_gid	GA1.1. 1101783526.1597101359	Google Analytics

These identification numbers contain the UNIX timestamp at the end, which indicates when the respective cookie was set for the first time. The identification number with the UNIX timestamp "1597101359" was set on Tuesday 11 August 2020 at 01:15:59 CET.

The same values as in the cookie files "_ga" and "gid" were included in the request payload for the domain www.google-analytics.com/collect (emphasis added by the DPA):

v=1&_v=j83&aip=1&a=757249675&t=pageview&_s=1&dl=https%3A%2F%2F&ul=de&Amp;
de=windows-1252&dt=████████%20%C3%96sterreich&sd=24—

bit&sr=1920x1080&vp=1903x910&je=0&fl=32.0%20r0&_u=QACAAAAAB~&jid=&gjid=&cid=
165363541.1597101359 &tid=UA-109732782-
1&_gid=1101783526.1597101359&cd1=Home&z=339628709

These identification numbers make it possible for the respondents to distinguish website visitors and also to obtain information as to whether they are a new or a recurring website visitor to <http://www.████████.at/> www.████████.at.

In addition, the following information (parameter) was also sent to the second respondent via the complainant's browser in the course of inquiries (requests) to <https://www.google-analytics.com/collect> (excerpt from the HAR file, Request URL https://www.google-analytics.com/collect <https://www.google-analytics.com/collect>, excerpt of the request with time stamp 2020-08—11T01:26:23.795+02:00):

General

- Request URL https://www.google-analytics.com/collect
- Request Method GET
- HTTP version HTTP/2
- Remote address 2a00:1450:4016:807:200e

Headers

- Accept: */*
- Accept-encoding: gzip, deflate, br
- Accept-language: de,en;q=0.5
- Connection: keep-alive
- Content-Length: 303
- Content-type: text/plain;charset=UTF-8
- DNT: 1
- Host: www.google-analytics.com
- Origin: [https://\[REDACTED\].at](https://[REDACTED].at)
- Referer: [https://\[REDACTED\].at/](https://[REDACTED].at/)
- TE: Trailers
- User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0

Size

- Headers 677 bytes
- Body 0 bytes
- Total 677 bytes

From these parameters, it is possible to draw conclusions about the browser used, the browser settings, language selection, the website visited, the color depth, the screen resolution and the AdSense link number.

The remote address (IPV6 address) 2a00:1450:4016:807:200e is that of the second respondent.

The IP address of the complainant's device is transmitted to the second respondent in the context of these

inquiries to <https://www.google-analytics.com/collect>.

The content of the HAR file (Annex/4), submitted by the complainant with submission of 18 August 2020, is based on the findings of fact.

Assessment of evidence relating to C.8.: *The findings made are based on the complainant's submission of 18 August 2020 and the HAR file submitted therein, Supplement No/4. A HAR file is an archive format for HTTP transactions. The HAR file has been checked by the Data Protection Authority. The complainant's submissions are in line with the archive data contained therein. The submitted HAR file (or its contents) is known to the parties concerned. In addition, the findings made are based on the complainant's comments of 13 August 2021 and the screenshots contained therein. As stated above, according to the second respondent, the purpose of the identification numbers is to distinguish users. The established dates of cookie setting are calculated from the respective UNIX timestamps. The Unix time is a time definition developed for the Unix operating system and set as the POSIX standard. The Unix time counts the past seconds since Thursday, January 1, 1970, 00:00 UTC. The finding with regard to the remoteaddress results from an official Who Is query by the DPA at <https://ipinfo.io/2a00:1450:4016:807::200e> (requested 18 March 2022).*

C.9. Insofar as the Google Analytics tool is implemented on a website, the second respondent has the technical possibility to obtain the information that a particular Google account user has visited this website (on which Google Analytics is implemented), provided that this Google account user is logged in to the Google account during the visit.

Assessment of evidence relating to C.9.: *In its opinion of 9 April 2021 in parallel proceedings with the JCC: DSB-D155.027 admittedly argued in question 9 that he receives such information only if certain conditions are met, such as the activation of specific settings in the Google account. In the view of the DPA, this argument is not convincing. If a Google account user's wish for "personalisation" of the advertising information received can be met on the basis of a declaration of intent in the account, it is possible, from a purely technical point of view, to obtain the information on the visited website of the Google Account user. In this context, there is an explicit reference to data protection accountability, which will be discussed in more detail in the legal assessment. For the purpose of establishing the facts, this data protection accountability means that the respondent (or, in any case, the first respondent as controller)— and not the complainant or the data protection authority— must provide sufficient evidence. Such sufficient evidence — i.e. that there is no possibility of obtaining data for the second respondent from a technical point of view — was not provided in this context, especially since it is precisely an essential part of the concept of Google Analytics to be implemented on as many websites as possible in order to be able to collect data. As can be seen from the legal assessment, such a reversal of the burden of proof is expressly provided for in the GDPR.*

C.10. The first respondent <http://www.█████.at/> removed the Google Analytics tool from its website

www.█████.at before the outcome of the proceedings at issue.

Assessment of evidence in relation to C.10.: The findings are based on the opinion of the first respondent of 28 May 2021, which was not disputed by the complainant in this respect. In addition, the finding is based on an official search at www.█████.at (requested 18 March 2022).

D. From a legal point of view, it follows:

D.1. General information

a) On the competence of the data protection authority

The European Data Protection Board (hereinafter: EDPB) has already dealt with the relationship between GDPR and Directive 2002/58/EC ("e-Privacy Directive") (cf. Opinion 5/2019 on the interaction between the e-Privacy Directive and the GDPR of 12 March 2019).

By decision of 30 November 2018, ZI. DSB-D122.931/0003-DSB/2018, with the relationship between GDPR and the national implementing provision (in Austria now: TKG 2021, BGBI. I No 190/2021 as amended).

It was stated in principle that the e-Privacy Directive (or the respective national implementing provision) of the GDPR acts as *lex specialis*. Thus, Article 95 of the GDPR provides that the Regulation does not impose any additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services on public communications networks in the European Union, in so far as they are subject to specific obligations laid down in the e-Privacy Directive which pursue the same objective.

However, the e-Privacy Directive does not contain any obligations within the meaning of Chapter V of the GDPR in the event of the transfer of personal data to third countries or international organisations.

Against this background, the GDPR is applicable to such a data transfer and therefore the data protection authority has competence to deal with the present complaint pursuant to Art. 77 para. 1 GDPR.

b) Article 44 GDPR as subjective right

On the basis of the previous case-law of the data protection authority and the courts, it should be noted that both the lawfulness of data processing pursuant to Article 5(1)(a) in conjunction with Article 6 et seq. of the GDPR and the rights of data subjects postulated in Chapter III of the Regulation can be asserted as subjective right in the context of a complaint pursuant to Article 77(1) GDPR.

The transfer of personal data to a third country which does not guarantee an adequate level of protection within the meaning of Article 44 of the GDPR (as claimed) has not yet been the subject of a complaint procedure before the data protection authority.

In this context, it should be noted that Article 77(1) of the GDPR (and, moreover, also the national provision of Section 24(1) of the DSG) for the exercise of the right of appeal requires only *that “the processing of personal data concerning them infringes this Regulation”*.

In its judgment of 16 July 2020, the Court of Justice also held that the finding that '*[i]n the law and practice of a country does not guarantee an adequate level of protection*', and that '*[t]he compatibility of this (adequacy) decision with the protection of privacy and the freedoms and fundamental rights of persons* may be invoked as a subjective right *in the context of a complaint under Article 77(1) of the GDPR* (cf. *judgment of the Court of Justice of 16 July 2020, C-311/18, paragraph 158*).

Admittedly, it should be noted that the question referred for a preliminary ruling in the abovementioned proceedings did not concern the ‘scope of the right of appeal under Article 77(1) of the GDPR’; however, the ECJ has clearly considered the fact that an infringement of provisions of Chapter V GDPR can also be invoked in the context of a complaint under Article 77(1) GDPR as a necessary condition. From a different perspective, the CJEU would have stated that the question of the validity of an adequacy decision cannot be resolved at all in the context of a complaint procedure.

To the extent that the second respondent also asserts Article 44 GDPR as a subjective right — with reference to the wording of ErwGr 141 leg.cit. — denies that the above-mentioned ErwGr refers to the fact that the ‘rights under this regulation’ are accessible to a complaint under Article 77(1) of the GDPR (and not: “the rights referred to in Chapter III of this Regulation”).

While the GDPR uses the term ‘rights of a data subject’ at certain points, this does not mean, conversely, that no other norms in which this wording is chosen can also be invoked as subjective law. Most of the provisions of the GDPR are, on the one hand, an obligation of the controller (and partly the processor), but on the other hand can also be invoked as a subjective right to data subjects. For example, it is undisputed that Articles 13 and 14 of the GDPR establish a subjective right of information, even though the right to information is not mentioned in Article 12(2) of the GDPR as “their rights” (i.e. “rights of the data subject”) and Article 13 and Article 14 GDPR are designed according to the wording as the information obligation of the person responsible.

The decisive factor is whether a data subject is affected by an alleged infringement in an individual legal position. The alleged infringement must therefore have a negative impact on and affect the person concerned.

Apart from that, although the ErwGr is an important tool for interpreting the GDPR, they cannot be used to achieve a result contrary to the text of the regulation (as stated above, the fact that the administrative remedy is generally linked to ‘processing’) (see the judgment of the Court of Justice of 12 May 2005 in Case C-444/03 paragraph 25 and the other case-law cited).

Finally, according to the national case-law of the VwGH, in the event of doubt, it must be assumed that

rules which require administrative action also and precisely in the interests of the person concerned grant him a subjective right, that is to say enforceable by means of a complaint (see, for example, VwSlg. 9151 A/1976, 10.129 A/1980, 13.411 A/1991, 13.985 A/1994).

In the light of the wording of Article 77(1) of the GDPR and the above-mentioned judicature of the CJEU and the VwGH, it should be noted that the obligation laid down in Chapter V and, in particular, the obligation for controllers and processors to ensure the level of protection for natural persons guaranteed by the Regulation can, conversely, also be asserted as subjective right before the competent supervisory authority pursuant to Article 77(1) GDPR.

c) On the competence of the data protection authority to determine

The complainant submitted observations of 11 February 2021 and 8 June 2021 in accordance with § 24(2)(5) DSG expressly requests a declaration that the Data transfers pursuant to Art. 44 GDPR were inadmissible.

According to the case-law of the VwGH and the BVwG, the data protection authority has a competence to determine breaches of the right to confidentiality in appeal proceedings (for example, the finding of the BVwG of 20 May 2021, ZI. W214 222 6349-1/12E; implicitly the finding of the VwGH of 23 February 2021, Ra 2019/04/0054, in which it dealt with the finding of a breach of professional secrecy in the past, without taking into account the lack of competence of the defendant authority).

There are no objective reasons to use the competence to determine the determination pursuant to Art. 58 para. 6 GDPR in conjunction with § 24 para. 2 point 5 GDPR and paragraph 5 of the DSG for the determination of an infringement of Art. 44 GDPR, since in the present case, among other things, an infringement of law that occurred in the past - namely a transfer of data to the USA — is generally linked to a violation of the GDPR in accordance with § 24 para. 1 DSG — as well as Article 77(1) GDPR.

If the ruling of a decision in a complaint procedure could contain only instructions under Article 58(2) GDPR, there would be no scope for § 24(2)(5) and 24(5) DSG as a result.

Contrary to the opinion of the respondents, Paragraph 24(6) of the DSG is not eligible for the subject-matter of the appeal which is relevant here, since a data transfer is cancelled in the past. In other words: The alleged injustice (here: Incompatibility with Art. 44 GDPR) of a data transfer that has already been completed is not accessible to a conclusion of the procedure pursuant to § 24 para. 6 DSG.

In the light of these considerations, it should be noted, as a further interim conclusion, that the DPA's powers of determination are present in the present appeal procedure.

d) “serious and far-reaching practical significance” of the present decision

In summary, the second respondent stated in its last observations of 9 February 2022 that a decision

granting the appeal would have serious economic consequences.

In this regard, it should be noted that the data protection authority is prohibited from economic or political considerations and that these considerations are to be taken into account only on a point-by-point basis in the context of the interpretation of the GDPR, for example in the context of a balancing of interests under Article 6(1)(f) of the GDPR.

In accordance with the primary law Art. 8(3) EU-GRC and the secondary law Art. 58(1)(f) GDPR, the Data Protection Authority has on the contrary the obligation to take a decision in the context of data protection complaints, taking into account the position of the Court of Justice in the judgment of 16 July 2020, Case C-311/18, with regard to the legal situation of the USA.

Thus, in its judgment of 16 July 2020, the CJEU expressly stated that the relevant legal situation in the USA — below — is not compatible with the fundamental right to data protection under Article 8 of the EU-CFR, which is why the EU-US adequacy decision ('Privacy Shield') was also declared invalid.

An economic or political agreement to ensure data transfers between Europe and the US has to be reached by other bodies, but not by supervisory authorities. The arguments put forward by the second respondent concerning the 'serious and far-reaching practical significance' of the decision in question and the economic studies cited must therefore be omitted.

D.2. Point 1

By decision of 2 October 2020, Zl. D155.026, 2020-0.526.838, pending the determination of which authority is responsible for the substantive conduct of proceedings (lead supervisory authority) or pending the decision of a lead supervisory authority or the EDPB.

In the opinion of the Data Protection Authority, Article 4(23)(b) GDPR is fulfilled, since the first respondent's online comparison portal [REDACTED] — as noted — on the Austrian (www.[REDACTED].at), German (www.[REDACTED].de), Polish ([http://www.\[REDACTED\].pl](http://www.[REDACTED].pl)) and English-speakingmarket (www.[REDACTED].eu) and is undisputed for all versions of [REDACTED] the website operator. Thus, the procedure under Article 56 in conjunction with Article 60 et seq. of the GDPR ('One-Stop-Shop') was to be conducted.

Subsequently, the data protection authority — as the lead supervisory authority — submitted a draft decision to the supervisory authorities concerned in accordance with Article 60(3) GDPR.

In the absence of any relevant and reasoned objections to the draft decision, the suspension decision of 2 October 2020 had to be corrected and communicated to the parties pursuant to Article 60(7) and (8) of the GDPR.

Since, of its own motion, decisions which do not give rise to a right to a person may be annulled or

altered by the authority which issued the decision or, in the exercise of the supervisory right, by the relevant higher authority, and as a result of a stay of proceedings by a party to the proceedings, no right to a non-decision arises, the above-mentioned decision of 2 October 2020 was also open to a remedy pursuant to Paragraph 68(2) of the AVG.

D.2. Point 2. (a)

a) General information on the concept of “personal data”

The material scope of Article 2(1) GDPR — and thus the success of this complaint — fundamentally presupposes that “personal data” are processed.

According to the legal definition of Article 4(1) GDPR, "*personal data is all information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more specific characteristics that can be identified as an expression of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person shall be regarded as identifiable*".

As can be seen from the findings of fact (see points C.3. and C.8.), the first respondent — as the operator of the website — implemented the tool Google Analytics on its website. As a result of this implementation — i.e. triggered by the JavaScript code executed during the visit to the website — at least the following information was transmitted to the second respondent's servers by the complainant's browser who visited the website www.█████.at:

- unique online identifiers that identify both the complainant's browser or device and the first respondent (through the first respondent's Google Analytics Account ID as website operator);
- the address and HTML title of the website and the subpages visited by the complainant;
- Information on the browser, operating system, screen resolution, language selection and date and time of the visit to the website;
- the IP address of the device used by the complainant.

It is necessary to verify whether this information falls within the definition of Article 4(1) GDPR, i.e. personal data of the complainant.

b) Identification numbers as “personal data”

With regard to the online identifiers, it should be recalled that the cookies “_ga” or “cid” (Client ID) and “_gid” (User ID) contain unique Google Analytics identification numbers and have been stored on the complainant's device or browser. As noted, it is possible for certain bodies — for example the respondents — to distinguish website visitors using these identification numbers and also to obtain information as to whether it is a new or a recurring website visitor to www.█████.at. In other words:

Only the use of such identification numbers allows a distinction between website visitors, which was not possible before this assignment.

In the opinion of the Data Protection Authority, an interference with the fundamental right to data protection pursuant to Article 8 EU-GRC and § 1 of the DSG already exists if certain bodies take measures — here the assignment of such identification numbers — in order to individualise website visitors in this way.

There is no need for a measure of “identifiability” in such a way that it must immediately be possible to associate such identification numbers with a specific “face” of a natural person, in particular the name of the complainant (see Opinion 4/2007, WP 136, 01248/07/EN of the former Article 29 Working Party on the concept of “personal data”, p. 16 f); see the guidance provided by the supervisory authorities for telemedia providers in March 2019, p. 15).

In favour of such an interpretation, ErwGr 26 GDPR argues that the question of whether a natural person is identifiable *takes into account all means likely to be used by the controller or another person in the general discretion to identify the natural person directly or indirectly, such as separating the natural person* “singling out”). The term ‘separate’ means ‘chosen from a set’ (see <https://www.duden.de/rechtschreibung/aussondern>, questioned on 18 March 2022), which corresponds to the above considerations on the individualisation of website visitors.

The literature also explicitly states that a “digital footprint” which allows devices to be clearly individualised — and subsequently the specific user — is already a personal date (cf. Karg in Simitis/Hornung/Spiecker, GDPR Comment Art. 4 Z 1 Rz 52 mwN). Due to the uniqueness of the identification numbers, this consideration can be transferred to the present case, especially since these identification numbers can also be combined with other elements — which is to be discussed in greater detail at once.

In so far as the respondents lead to the meeting that no “means” would be used to link the identification numbers at issue here with the complainant’s person, it should be pointed out again that the implementation of Google Analytics on www.█████.at results in <http://www.█████.at/> a separation within the meaning of the ErwGr 26 GDPR. In other words: If you use a tool that just allows such separation, it is not possible to take the view that, according to “general discretion”, no means should be used to make natural persons identifiable.

At this point, it should be noted that the European Data Protection Supervisor (EDPS) is also of the opinion that “separation” by marking a terminal device must be considered as a personal date. Thus, in his decision of 5 January 2022, the EDPS: 2020-1013 against the European Parliament, *inter alia*:

Tracking cookies, such as the Stripe and the Google analytics cookies, are considered personal data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection. All records containing identifiers that can be used to single out users, are

considered as personal data under the Regulation and must be treated and protected as such."

Tracking cookies such as Stripe and Google Analytics cookies are considered personal data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection. All data sets containing identification features that can be used to separate users are considered personal data under the Regulation and must be treated and protected as such" (translation by the DPA).

It is true that the EDPS is required to apply Regulation (EU) 2018/1725, which applies to data processing by the Union institutions, bodies, offices and agencies. However, since Article 3(1) of Regulation (EU) 2018/1725 corresponds to the definition of Article 4(1) of the GDPR, those considerations can easily be transposed to the present case.

As an interim result, it should therefore be noted that the Google Analytics identification numbers at issue here are already in principle to be qualified as personal data (in the form of an online identifier) in accordance with Art. 4 Z 1 GDPR.

c) Combination with other elements

The fulfillment of Article 4(1) GDPR becomes even clearer if one takes into account that such identification numbers can be combined with other elements:

By combining all these elements — that is, unique identification numbers and the other information mentioned above, such as browser data or IP address — it is all the more likely that the complainant can be identified (see again ErwGr 30 GDPR). Such a combination makes the complainant's "digital footprint" even more unique.

The respondents' arguments relating to the "anonymisation function of the IPaddress" may be omitted, since the complete IP address is processed at least for a certain — albeit very short — period on Google LLC's server. This short data processing period is sufficient to comply with Article 4(2) of the GDPR. According to the case-law of the BVwG, it cannot be inferred from Article 4(2) in conjunction with Article 6 GDPR that a certain 'minimum processing' must be assumed (cf. the finding of the BVwG of 3 September 2019, ZI. W214 2219944-1).

As will be explained later, this full IP address can be accessed by U.S. intelligence services, even if it was processed in the specific case, as claimed, on European servers of the second respondent.

Similarly, the question of whether an IP address is a personal date, viewed in isolation, may be left out, since — as mentioned — it can be combined with other elements (in particular the Google Analytics identification number). In this context, however, it should be noted that, according to the ECJ's case-law, the IP address may constitute a personal date (see the judgments of the Court of Justice of 17 June 2021, C-597/19, paragraph 102, and of 19 October 2016, C-582/14, paragraph 49), and that the IP address does not lose its status as a personal date solely because the means of identification lie with a third party.

d) Traceability to the complainant

However, irrespective of the above considerations, there must be no traceability to the complainant's 'face':

Indeed, it is not necessary for the respondents to be able to establish a personal connection on their own, that is to say that all the information necessary for identification is with them (cf. the judgments of the Court of Justice of 20 June 2006). December 2017, C-434/16, paragraph 31, and of 19 October 2016, C-582/14, paragraph 43). Rather, it is sufficient that anyone can — with legally permissible means and reasonable effort — make this personal reference (cf. Bergauer *in Jahnel*, GDPR comment Art. 4 Z 1 Rz 20 mVa *Albrecht/Jotzo*, *The new data protection law of the EU 58*).

Such an interpretation of the scope of Art. 4 Z 1 GDPR can be derived — in addition to the legal and literature sources mentioned — from ErwGr 26 GDPR, according to which, in the case of identification, not only the means of the person responsible (here: the first respondent) but also that of 'another person' (English version of the Regulation: "by another person"). This is also the result of the idea of providing data subjects with the greatest possible protection of their data.

In particular, the CJEU has also repeatedly stated that the scope of the GDPR should be understood "very broad" (see, for example, the judgments of the CJEU of 22 June 2021, C-439/19, paragraph 61; with regard to the comparable legal situation in that regard, the judgments of 20. December 2017, C-434/16, paragraph 33, and of 7 May 2009, C-553/07, paragraph 59).

It is not overlooked that according to ErwGr 26 GDPR it is also to be taken into account with which "probability" anyone uses means to identify natural person directly or indirectly. Indeed, in the view of the Data Protection Authority, the term 'someone' — and thus the scope of Article 4(1) of the GDPR — should not be interpreted so broadly that any unknown actor could theoretically have special knowledge in order to establish a personal relationship; this would result in almost any information falling within the scope of the GDPR and making it difficult or even impossible to distinguish it from non-personal data.

Rather, the decisive factor is whether identification can be made with reasonable and reasonable effort (see the decision of 5. December 2018, GZ DSB-D123.270/0009- DSB/2018, according to which personal data no longer exists if the controller or a third party can only establish a personal connection with a disproportionate effort).

In the present case, however, there are now certain actors who have a special knowledge which makes it possible to establish a connection with the complainant in the sense of the above and therefore to identify him.

i) This is, first of all, the second respondent:

As can be seen from the findings of fact, the complainant was logged in <http://www.████████.at/> with his

Google account at the time of the visit to the website www. [REDACTED].at. The second respondent has stated that the latter receives information due to the fact that the Google Analytics tool is implemented on a website. This includes information that a certain Google account user has visited a certain website (see comments of 9 April 2021, question 9).

This means that the second respondent received at least the information that a user logged in to the complainant's Google account visited the website www. [REDACTED].at.

Therefore, even if one takes the (not required) view that the above-mentioned online identifiers must be assigned to a certain "face", such assignment can in any case be made via the complainant's Google account.

It is not overlooked by the second respondent that certain conditions must be met for such an assignment, such as the activation of specific settings in the Google account (see again his opinion of 9 April 2021, question 9).

However, if, as the complainant has stated convincingly, the identification of a website visitor depends only on whether certain declarations of intent are made in the account, there are (from a technical point of view) all possibilities for identification. On a different perspective, the second respondent could not respond to a user's wishes expressed in the account settings for 'personalisation' of the advertising information received.

In this context, it is necessary to make explicit reference to the unequivocal wording of Article 4(1) of the GDPR, which is linked to a skill ('can be identified') and not to whether an identification is ultimately carried out.

Likewise, the accountability of the first respondent as enshrined in the GDPR — as the person responsible for this purpose, should be explicitly mentioned below — in accordance with Article 5(2) in conjunction with Article 24(1) in conjunction with Article 28(1) GDPR, in order to ensure and to be able to prove that the processing (with the assistance of a processor) is carried out in accordance with the Regulation. It is therefore a debt to bring.

This also includes proof that processing is currently not subject to the regulation, especially since the respondents have concluded data protection contracts in relation to Google Analytics, which in turn presuppose the applicability of the GDPR. However, such evidence was not provided, despite the possibilities granted several times.

Contrary to Chapter V — on this point below — Article 5(2) in conjunction with Article 24(1) of the GDPR is now actually based on a risk-based approach. The higher the risk associated with data processing, the higher the standard of evidence to be provided to demonstrate compliance with the GDPR.

In the present case, a high risk and therefore a high standard of proof must be assumed:

In any case, the second respondent developed the product Google Analytics in order to collect as much information as possible from website visitors. Thus, the latter himself states that due to the fact that Google Analytics is embedded on a website, it may receive the information that a certain Google account holder has visited such a website. In other words: In return for the fact that website operators can use the free version of Google Analytics, the second respondent will be given technical possibilities to collect data and further enrich Google account holders' profiles. It cannot therefore be assumed that Google Analytics is a mere web analysis service for website operators.

On the basis of this high standard of proof, it is not sufficient to merely claim that the second respondent receives the information at issue only if certain settings are selected in the Google account. Further evidence (such as screenshots, detailed technical descriptions, etc.) was not provided, despite an extensive investigation.

It is not overlooked that accountability pursuant to Art. 5 para. 2 in conjunction with Art. 24 para. 1 GDPR expressly affects the first respondent as responsible. However, the granting part of the decision in question is (only) directed against the first respondent, who embedded the product Google Analytics on her website.

In so far as the second respondent refers in this context to the presumption of innocence pursuant to Article 48(1) EU-GRC, it must be pointed out that, in the present case, it is exclusively a complaint procedure under Article 77(1) GDPR and not an administrative criminal procedure. Apart from that, the appeal against the second respondent was dismissed.

Finally, if the second respondent states that such a 'distribution of burden of proof' is incompatible with Austrian procedural law, it must be pointed out to him that such a distribution is quite common in the legal order — in particular in consumer protection law — (see, for example, Paragraph 924 of the ABGB or § 11(1) VGG, BGBl. I No 175/2021; the close relationship between the Consumer protection law and the fundamental right to data protection see also ErwGr 42 GDPR).

ii) Regardless of the second respondent, however, and this is of greater relevance on a case-by-case basis, the U.S. authorities must be taken into account:

As the complainant has just as rightly pointed out, US intelligence services take certain Online identifiers (such as: the IP address or unique Identification numbers) als Starting point for monitoring from individuals. In this way, in particular: not it is ruled out that these intelligence services have already collected information that allows the data transmitted here to be traceable to the complainant's person.

The fact that this is not merely a 'theoretical threat' is apparent from the judgment of the Court of Justice of 16 July 2020, C-311/18, which ultimately declared the EU-US adequacy decision ('Privacy Shield')

invalid because of the incompatibility of such methods and possibilities of access by the US authorities with the fundamental right to data protection under Article 8 of the EU-GRC.

In particular, this can also be seen in the second respondent's transparency report, referred to in the findings of fact, which demonstrates that requests for data from US authorities to the second respondent are made. For example, metadata and content data can be requested from the second respondent.

Admittedly, it is not overlooked that the first respondent is of course not able to verify whether such access by US authorities occurs on a case-by-case basis — i.e. per website visitor — and which information is already available by US authorities; conversely, this circumstance cannot be blamed on persons such as the complainant. It was ultimately the first respondent as a website operator who — despite the publication of the aforementioned judgment of the CJEU of 16 July 2020 - continued to use the Google Analytics tool.

Specifically, therefore, the information was provided that the complainant, with a terminal device marked with a unique Google Analytics identification number, at a certain point in time with certain browser settings and a specific IP address, is a specific website (here: a comparison portal in the form of [REDACTED]).

It is true, in principle, that this is (at first) only information about a particular terminal device. However, just as the location data of a vehicle obtained by means of a GPS tracker may at the same time also constitute personal data on the driver's stay, the relevant information here constitutes personal data of the person most likely to use the terminal device.

This is the complainant's case in the present case, especially since he was (indisputably) logged in with the personal Google account in the browser at the time of accessing the website. There are no indications that the complainant has handed over his access data to third parties and, as far as can be seen, has not been claimed by any party.

A measure to the effect that "security" has to be determined which natural person has used the terminal device cannot be derived from Art. 4(1) GDPR and is not required either:

In this regard, information belonging to an end device or an account would always be non-personal data, since in principle it can never be ruled out that the terminal device or access data has been passed on to third parties (such as friends or family members). Such a view would lead to a too narrow scope of application of Article 4(1) GDPR, which in turn contradicts the ECJ's judicature, which assumes a very broad scope.

As a further interim conclusion, it should therefore be noted that the information mentioned in the findings of fact under C.8 (in combination in any case) is personal data in accordance with Art. 4 Z 1 GDPR.

e) Role distribution

As already stated, the first respondent, as a website operator, took the decision to implement the Google Analytics tool on <http://www.█████.at>"the website www.█████.at. Specifically, it has inserted a JavaScript code ('tag') provided by the second respondent in the source code of her website, thereby running this JavaScript code when visiting the website in the complainant's browser. In this regard, the first respondent stated that the above-mentioned tool is used for statistical analysis of the behaviour of website visitors (see the comments of 22. December 2020, question 2).

As a result, the first respondent decided on the "purposes and means" of the data processing associated with the tool, which is why this (in any case) is to be regarded as the controller within the meaning of Art. 4 Z 7 GDPR.

As regards the second respondent, it should be noted that the subject-matter of the appeal in this case relates (only) to the transfer of data to the second respondent to the USA. A possible further processing of the information referred to in the findings of fact under C.8 (by Google Ireland Limited or the second respondent) is not subject to appeal and has therefore not been determined in this direction.

The data protection role of the second respondent is therefore no longer relevant to the proceedings at issue, especially since the obligation to comply with Article 44 GDPR applies equally to controllers and processors.

D.3. Point 2. (b)

a) Scope of Chapter V GDPR

First, it is necessary to verify whether the first respondent is subject to the obligations laid down in Chapter V of the Regulation.

Pursuant to Article 44 of the GDPR, any *transfer of personal data which is already being processed or which is to be processed after its transfer to a third country or an international organisation is permitted only if the controller and the processor comply with the conditions laid down in this Chapter and that the other provisions of this Regulation are also complied with; this shall also apply to any onward transfer of personal data from the third country or international organisation concerned to another third country or international organisation. All provisions of this Chapter shall be applied in order to ensure that the level of protection afforded to natural persons by this Regulation is not undermined.'*

In ‘Guidelines 5/2021 on the relationship between the scope of Article 3 and the requirements for international traffic pursuant to Chapter V of the GDPR’ (currently still in public consultation), the EDPB identified three cumulative conditions as to when there is a ‘transmission to a third country or an international organisation’ within the meaning of Article 44 of the GDPR (*ibid.* paragraph 7):

- the controller or processor is subject to the GDPR for the processing in question;
- the controller or processor ('data exporter') discloses, by transfer or otherwise, personal data which are the subject of such processing to another controller, a joint controller or a processor ('data importer');
- the data importer is located in a third country or is an international organisation, whether or not that data importer is subject to the processing in question pursuant to Article 3 of the GDPR.

The first respondent is based in Austria and is responsible for the operation of the website www.█████.at data protection law. In addition, the first respondent (as a data exporter) disclosed personal data of the complainant by proactively implementing the Google Analytics tool on its website www.█████.at <http://www.█████.at/> and by transmitting data to the second respondent (to the USA) as a direct consequence of this implementation. Finally, the second respondent has its registered office in the USA.

Since all the conditions set out in the EDPB guidelines are met, the first respondent, as the data exporter, is subject to the provisions of Chapter V of the Regulation.

b) Rules of Chapter V GDPR

Subsequently, it is necessary to verify whether the transfer of data has taken place in accordance with the requirements of Chapter V of the GDPR to the USA.

Chapter V of the Regulation provides for three instruments to ensure the adequate level of protection required by Article 44 of the GDPR for data transfers to a third country or an international organisation:

- Adequacy decision (Art. 45 GDPR);
- Appropriate safeguards (Art. 46 GDPR);
- Exceptions for certain cases (Art. 49 GDPR).

c) Adequacy decision

The CJEU has ruled that the EU-US adequacy decision ('Privacy Shield') is invalid without maintaining its effect (see judgment of 16 July 2020, C-311/18, paragraphs 201 f).

The data transmission in question is therefore not covered by Art. 45 GDPR.

d) Appropriate safeguards

As can be seen from fact finding C.5, the respondents have standard data protection clauses (as follows: SDK) pursuant to Art. 46 para. 2 lit. c GDPR for the transfer of personal data to the USA ("Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses". Specifically, at the time of appeal, those clauses were those as amended by Commission Implementing Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors in third countries pursuant to Directive 95/46/EC of the European Parliament and of the Council, OJ 2010/39, p. 5.

In the aforementioned judgment of 16 July 2020, although the CJEU stated that SDK as an instrument for international data traffic could not be criticised, the CJEU also pointed out that SDK by its very nature is a treaty and therefore cannot bind authorities from a third country:

'It follows that there are situations in which, in the light of the legal situation and practice in the third country concerned, the recipient of such a transfer can guarantee the necessary data protection solely on the basis of the standard data protection clauses, but also situations in which the arrangements contained in those clauses may not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, for example, if the law of that third country allows its authorities to interfere with the rights of data subjects with regard to that data' (ibid. paragraph 126).

However, a more detailed analysis of the legal situation of the USA (as a third country) may not be carried out at this point, as the CJEU has already dealt with it in the above-mentioned judgment of 16 July 2020. It concluded that the EU-US adequacy decision does not provide an adequate level of protection for natural persons under the relevant US law and the implementation of official monitoring programmes, *inter alia* based on section 702 of the FISA and E.O. 12333 in conjunction with the PPD-28 (ibid. paragraph 180 et seq.).

These considerations can be applied to the present case:

For the data protection authority, there is no doubt that the second respondent is to be qualified as an electronic communications service provider within the meaning of 50 U.S. Code § 1881(b)(4) and is therefore subject to supervision by US intelligence services pursuant to 50 U.S. Code § 1881a ("FISA 702"). Accordingly, the second respondent has an obligation to provide the US authorities with personal data pursuant to the 50 U.S. Code § 1881a.

As is apparent from the second respondent's Transparency Report, such requests are also regularly made by US authorities to the latter ([seehttps://transparencyreport.google.com/user-data/us-national-security?hl=en](https://transparencyreport.google.com/user-data/us-national-security?hl=en), questioned on 18 March 2022).

Against this background, in its judgment of 16 July 2020, the CJEU also stated that '*standard data protection clauses cannot, by their very nature, provide guarantees that go beyond the contractual obligation to ensure compliance with the level of protection required by EU law*' and that '[t]he situation

in a given third country may require the controller to take additional measures to ensure compliance with that level of protection' (ibid., paragraph 133).

The data transmission in question cannot therefore be based solely on the standard data protection clauses concluded between the respondents (cf. Art. 46(2)(c) GDPR).

e) General information on “additional measures”

In its ‘Recommendations 01/2020 on measures to supplement transfer tools to ensure the level of protection of personal data under Union law V. 2.0’, the EDPB stated that if the law of the third country affects the effectiveness of appropriate safeguards (such as SDK), the data exporter must either suspend the transfer of data or implement additional measures (ibid. paragraphs 28 et seq.).

Such “additional measures” within the meaning of the judgment of the CJEU of 16 July 2020 may be contractual, technical or organisational according to the recommendations of the EDPB (ibid. paragraph 52):

With regard to contractual measures, it is stated that “[t]he guarantees provided by the transfer tool and the relevant legislation in the third country do not meet all the conditions necessary to ensure a level of protection which is substantially equivalent to that in the EU, taking into account all the circumstances of the transfer. As the nature of the contractual measures cannot bind the authorities of the third country in general if they are not party to the contract, they must be combined with other technical and organisational measures in order to ensure the necessary level of data protection. The mere fact that one or more of these measures have been selected and applied does not necessarily mean that it is systematically ensured that the intended transfer meets the requirements of EU law (granting an essentially equivalent level of protection)' (ibid., paragraph 99).

With regard to organisational measures, it is stated that “[...]” may be internal strategies, organisational methods and standards that the controllers and processors could apply to themselves and impose on data importers in third countries. Depending on the particular circumstances of the transfer and the assessment of the legal situation in the third country, organisational measures to supplement the contractual and/or technical measures are necessary to ensure that the protection of personal data is substantially equivalent to the level of protection afforded in the EEA (ibid. paragraph 128).

As regards technical measures, the aim is to ensure that "the access of authorities in third countries to the data transmitted does not undermine the effectiveness of the appropriate safeguards referred to in Article 46 GDPR. Even if access by the authorities is in accordance with the law in the country of the data importer, these measures must be considered if access by the authorities goes beyond what constitutes a necessary and proportionate measure in a democratic society. These measures aim to exclude potentially infringing access by preventing public authorities from identifying, accessing information about data subjects, identifying them in other contexts or linking the data transmitted to other

datasets, including data on online identifiers of devices, applications, tools and protocols used by data subjects in other contexts (*ibid.* paragraph 79).

Finally, the EDPB stated that such ‘additional measures’ should be regarded as effective within the meaning of the judgment of 16 July 2020 only if and to the extent that the measure precisely fills the legal gaps identified by the data exporter in his examination of the legal situation in the third country. If the data exporter is ultimately unable to achieve a substantially equivalent level of protection, he or she may not transfer the personal data’ (*ibid.* paragraph 75).

With regard to the present case, this means that it is necessary to examine whether the “additional measures taken” by the second respondent close the gaps in legal protection identified in the ECJ judgment of 20 June 2020, i.e. the access and monitoring possibilities of US intelligence services.

f) **‘Additional measures’ of the second respondent**

The second respondent has now implemented various measures in addition to the conclusion of the SDK (see its observations of 9 April 2021, question 28).

With regard to the contractual and organisational measures set out above, it is not clear to what extent notification of data requests to the data subject (should this be permissible in individual cases), the publication of a transparency report or a “directive for dealing with government requests” are effective in the sense of the above considerations. It is also unclear to what extent the “careful examination of any request for access to data” constitutes an effective measure, since in the aforementioned judgment of 20 June 2020 the CJEU ruled that admissible (i.e. legal) requests from US intelligence services are not compatible with the fundamental right to data protection under Article 8 of the EU Charter.

As far as the technical measures are concerned, it is also not clear — and the Respondent has also not explained — to what extent the protection of communications between Google services, the protection of data in transit between data centres, the protection of communications between users and websites or an “on-site security” actually prevent or restrict the access of US intelligence services on the basis of US law.

If the second respondent subsequently refers to encryption technologies, such as the encryption of ‘rest data’ in the data centres, the EDPB’s recommendations 01/2020 should be re-committed to the respondent. It states that a data importer (such as the second respondent) subject to 50 U.S. code § 1881a (‘FISA 702’) has a direct obligation to grant access to it or to release it, as regards imported data held or held in his possession or under his control. This obligation may also explicitly cover cryptographic keys without which the data are not readable (*ibid.* paragraph 81).

As long as the second respondent thus has the possibility of accessing data in plain language, the technical measures introduced at the meeting cannot be considered effective in the sense of the above

considerations.

The second respondent argues that, as a further technical measure, the meeting states that '*to the extent that ... Google Analytics data are personal data for the measurement of website owners, they must be regarded as pseudonymous*' (see its opinion of 9 April 2021, p. 26).

However, this is counteracted by the German Data Protection Conference's convincing view that "*the fact that users are made identifiable by means of IDs or identifiers does not constitute a pseudonymisation measure within the meaning of the GDPR. In addition, these are not appropriate safeguards to comply with data protection principles or to safeguard the rights of data subjects when IP addresses, cookie IDs, advertising IDs, unique user IDs or other identifiers are used to (re)recognise users. This is because, unlike in cases where data is pseudonymised in order to conceal or delete the identifying data so that the data subjects can no longer be addressed, IDs or identifiers are used to make individual individuals distinguishable and addressable. Consequently, there is no protective effect. These are therefore not pseudonymisations within the meaning of ErwGr 28, which reduce the risks to data subjects and help controllers and processors to comply with their data protection obligations*

 (see guidance provided by the supervisory authorities for telemedia providers in March 2019, p. 15).

Moreover, the second respondent's argument cannot be accepted either because the Google Analytics identifier — as explained above — can be combined with other elements and even linked to a Google account which is undisputedly attributable to the complainant.

The "anonymisation function of the IP address" is not effective, as the data is processed at least for a certain period by the second respondent, as explained above. Even assuming that the IP address was processed within the period only in servers in the EEA, it should be noted that under the relevant US law, the second respondent may nevertheless be obliged by US intelligence services to provide the IP address (see in detail the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex) of 10 July 2019, p. 1 f.).

Apart from this, the IP address is, in any case, only one of many "puzzle parts" of the complainant's digital footprint.

As a further interim conclusion, it should therefore be noted that the 'additional measures' at issue are not effective, since they do not close the legal protection gaps identified in the judgment of the CJEU of 20 June 2020, i.e. the access and monitoring possibilities of US intelligence services.

The data transmission in question can therefore not be covered by Art. 46 GDPR.

D.4. Point 2.(c)

a) Article 49 GDPR

According to the first respondent's own statements, the exception pursuant to Article 49 of the GDPR was not relevant to the data transfer in question (cf. the opinion of 16. December 2020).

Consent pursuant to Art. 49 para. 1 lit. a GDPR has not been obtained. Nor is it clear to the data protection authority how any other offence under Art. 49 GDPR should be fulfilled.

The data transfer in question cannot therefore be based on Art. 49 GDPR.

b) Chapter V GDPR does not know a risk-based approach

The second respondent further submits — in summary — that the risk of data transfer to the US must be taken into account and that the authority in question is too strict. It is not appropriate to follow these arguments:

Such a “risk-based approach” cannot be derived from the wording of Article 44 GDPR:

Art. 44 GDPR

General principles of data transmission

Any transfer of personal data which is already being processed or which is to be processed after its transfer to a third country or an international organisation shall be permitted only if the controller and the processor comply with the conditions laid down in this Chapter and comply with the other provisions of this Regulation; this shall also apply to any onward transfer of personal data from the third country or international organisation concerned to another third country or international organisation. All provisions of this Chapter shall be applied in order to ensure that the level of protection afforded to natural persons by this Regulation is not undermined.

Rather, it must be inferred from the wording of Article 44 GDPR that every data transfer to a third country (or an international organisation) must be ensured that the level of protection guaranteed by the GDPR is not undermined.

The outcome of an infringement of Article 44 GDPR does not therefore depend on whether there is a certain “minimum risk” or whether US intelligence services have actually accessed data. According to the wording of this provision, an infringement of Article 44 GDPR already exists when personal data are transferred to a third country without a corresponding level of protection.

In the context of those provisions of the GDPR, where a risk-based approach is actually to be adopted (“the higher the processing risk, the more measures to be implemented”), the legislator has also explicitly and without doubt regulated this. For example, the risk-based approach is provided for in Article 24(1) and (2), Article 25(1), Article 30(5), Article 32(1) and (2), Article 34(1), Article 35(1) and (3) or Article

37(1)(b) and (c) GDPR.

Since the legislator has standardised a risk-based approach in many parts of the GDPR, but not in connection with the requirements of Article 44 GDPR, it cannot be assumed that the legislator has merely ‘overlooked’ this; an analogous application of the risk-based approach to Art. 44 GDPR is therefore excluded.

Also the reference on the ‘free movement of data’ means: for the point of view of the Second respondent nothing to win:

It is completely undisputed that the GDPR should (also) guarantee the free movement of data. However, the free flow of data is under the premise that the provisions of the GDPR — including Chapter V — are fully complied with. There is no provision for softening in the sense of an “economically friendly interpretation” of the provisions of Chapter V in favour of the free movement of data. Economic interests were also irrelevant in the aforementioned judgment of the CJEU of 16 July 2020.

The further argument that the “risk-based approach was confirmed by the CJEU in its judgment of 16 July 2020” cannot be understood:

In its analysis of the legal situation of the US and the validity of the EU-US adequacy decision, the ECJ did not assume a risk-based approach in Chapter V GDPR. In fact, such a risk-based approach is not mentioned in the aforementioned judgment.

The second respondent seems to derive a risk-based approach from the words ‘adequate level of data protection’ used by the ECJ. This cannot be accepted, as the ECJ used this sequence of words with reference to ErwGr 108 GDPR. It is clear from ErwGr 108 of the Regulation that ‘adequate level of data protection’ means that the rights of data subjects must be respected in an appropriate manner.

With regard to the legal situation of the US, the CJEU has now just assumed that due to the disproportionate access possibilities of US authorities, no “adequate level of data protection” can be assumed, which is why it has finally declared the EU-US adequacy decision to be invalid.

The CJEU has not explicitly considered that the obligations to which a US-certified company is subject to a Privacy Shield may nevertheless be appropriate on a case -by-case basis (for example, because the certified company receives only non-sensitive or non-criminal relevant personal data).

Similarly, the argument that the European Commission in its Implementing Decision (EU) 2021/914, which adopted new standard contractual clauses, ‘also clearly advocated a risk-based approach’ cannot be understood:

It should be noted that Implementing Decision (EU) 2021/914 does not include a risk-based approach. The present implementing decision, adopted following the judgment of the Court of Justice of 16 July

2020, presupposes, on the contrary, that, in accordance with Article 14 thereof, the contracting parties to standard data protection clauses must now review the local laws and obligations in the case of access to the data by public authorities prior to the transfer of data to a third country.

In so far as the second respondent derives the alleged position of the European Commission from the (non-binding) ErwGr 20 of the abovementioned Implementing Decision, it must be pointed out that, even in ErwGr 20, no risk-based approach is assumed:

ErwGr 20 of that Implementing Decision correctly seeks to ensure that, when assessing the level of data protection in a third country, account must be taken, in particular, of the circumstances of the transfer.

Based on the example of the legal situation of the USA, it is necessary to verify, for example, whether in individual cases data is transmitted to an provider of electronic communications services within the meaning of 50 U.S. Code § 1881(b)(4), otherwise the corresponding access possibilities of according to FISA 702 are not applicable. If Austria were a third country, it would be necessary to check before data transfers to Austria whether the specific types of data transmitted, for example, fall within the scope of the (now) State Protection and Intelligence Service Act, BGBl. I No 5/2016, as amended, and whether the access possibilities of the Directorate for State Protection and Intelligence Service are proportionate.

However, this is (only) an examination of whether the local legislation and obligations in the case of access by public authorities to the data conflict with the contractual obligations of the standard data protection clauses and not a risk-based approach in the sense that it is necessary to verify how sensitive or non-sensitive the personal data transferred are.

Moreover, it should be noted that an implementing decision of the European Commission could not in any way impute a completely new content to the requirements of Article 44 of the GDPR (see, for example, on the primacy of the text of the regulation, the judgment of the Court of Justice of 12 May 2005, C-444/03, paragraph 25).

Finally, the reference to EDPB Recommendation 01/2020 on measures to supplement transmission tools to ensure the level of protection of personal data under EU law cannot help the second respondent's position:

Thus, as already pointed out in the context of Implementing Decision (EU) 2021/914, the body of the recommendations cited by the second respondent merely states that it is necessary to verify, for each transfer of data, whether the problematic laws of the third country are applied and precisely that it is not necessary to verify the sensitivity or non-sensitive nature of the personal data transferred.

Finally, in so far as the second respondent submits that U.S. intelligence services have no interest in the data processed at all — for example by stating that the information on “screen resolution is an industry standard” — it must be pointed out that it is not a matter of any interest of US intelligence

services, but rather of their means of access.

However, it should be noted that the added value of the information lies in the fact that it can be combined (see also the definition of “fingerprinting” in the Internet Architecture Board RFC6973, according to which “fingerprinting” is the process in which an observer identifies a device or an application body with sufficient probability on the basis of several information elements). For example, the IP address processed — as part of the digital footprint — can be used to determine which internet provider is being used and in which region the user of the device is present.

B) Result

Since an instrument of Chapter V of the Regulation does not guarantee an adequate level of protection for the data in question by the first respondent to the second respondent (in the USA), there is an infringement of Article 44 of the GDPR.

The first respondent was (at any event)<http://www.█████.at/> responsible for the operation of the website www.█████.at at the time of the appeal, namely 14 August 2020. The relevant data protection breach of Art. 44 GDPR is therefore attributable to the first respondent.

It was therefore appropriate to rule on the matter.

D.5. Remedial powers

In the opinion of the Data Protection Authority, the Google Analytics tool (in any case in the version of 14 August 2020) cannot therefore be used in accordance with the requirements of Chapter V GDPR.

However, since the Google Analytics tool was removed from the first respondent’s website before the conclusion of the appeal proceedings at issue, no recourse could be made to the remedies.

D.6. Point 3

It is necessary to verify whether the Second Respondent (as a data importer) is also subject to the obligations laid down in Chapter V of the Regulation.

On the basis of the above EDPB Guidelines 5/2021, it should be recalled that a transfer to a third country or an international organisation" within the meaning of Article 44 GDPR exists only if, *inter alia*, the controller or processor (data exporter) discloses personal data which are the subject of such processing to another controller, a joint controller or a processor (data importer) by transfer or otherwise.

This condition does not apply to the second respondent in the present case, since the latter (as a data importer) does not disclose the complainant’s personal data but receives them (only). In other words: The requirements of Chapter V GDPR are to be complied with by the data exporter, but not by the data

importer.

It is not overlooked by the complainant's reasoning that data transmission necessarily requires a recipient and that the second respondent (from a technical point of view) is part of the data transmission. However, it should be pointed out that data protection responsibility can still be "shared" (from a legal point of view) in the case of a processing operation, i.e. there may be a different degree of responsibility depending on the stage of the processing operation (cf. EDPB Guidelines 7/2020 on the concept of controllers and processors, paragraph 63 et seq.).

The data protection authority therefore considers that there is no infringement of Article 44 GDPR by the second respondent.

It was therefore appropriate to rule on the whole.

Finally, it should be pointed out that the second respondent's second respondent's question of the (possible) infringement of Article 5 et seq. in conjunction with Article 28(3)(a) and Article 29 of the GDPR is discussed with a further decision.

GZ: D155.008

Sachbearbeiterin: [REDACTED]

Complaint (Art. 77 DSGVO)
[REDACTED]**FINAL DECISION**Subject: Closing of proceeding

The complainant, Mr [REDACTED] [REDACTED], claimed in his complaint to the Hessian Commissioner for Data Protection and Freedom of Information of 26 January 2019, which was supplemented by a letter of 24 April 2019, an infringement of his right to erasure by the opponent, [REDACTED].

The opponent declared in its statement of 18 June 2019 that he complied with the complainant's request for erasure, which eliminated the alleged infringement.

The complainant was granted his right to be heard. While he did not deny the receipt of the opponent's statement, he did not make any further submissions despite being requested to do so.

Accordingly, the proceedings were closed.

20. July 2022

For the head of the Austrian data protection authority:
[REDACTED]

GZ: D155.073
2022-0.486.068

Sachbearbeiterin: [REDACTED]

Complaint (Art. 77 GDPR)

[REDACTED] (A61 VMN 318627)

FINAL DECISION

Subject: Closing of proceeding

The complainant [REDACTED] filed a complaint against [REDACTED] (opponent), which was submitted to the Austrian Data Protection Authority (DSB) by the Bavarian State Office for Data Protection Supervision (BayLDA) on August 20th 2021. An addition to the complaint was submitted on April 6th 2022.

The DSB forwarded the complaint to the opponent for comments. A copy of the statement of the controller from May 3rd 2022 was sent to the complainant by the BayLDA. Despite being given the opportunity to do so, the complainant did not submit any further comments.

Due to the reaction of the opponent, the complaint is considered to be settled. This is particularly due to the fact that the user account in question has been terminated and thus all personal data of the complainant has been deleted.

Accordingly, the proceeding is to be discontinued.

11. Juli 2022

Für die Leiterin der Datenschutzbehörde:

[REDACTED]

GZ: D155.066
2022-0.478.224

Barichgasse 40-42
A-1030 Vienna
Tel.: + 43-1-52152 [REDACTED]

E-mail: dsb@dsb.gv.at

Clerk: [REDACTED]
[REDACTED]
[REDACTED]

Data protection complaint (§ 24 DSG)

[REDACTED] (A56ID 318904)

by e-mail: [REDACTED]

Subject: Final Decision; Closing of the proceedings

On 3 February 2021, complainant [REDACTED] filed a complaint against [REDACTED] (respondent) to the Data Protection Authority, alleging a breach of the right to object by not responding to her request in this regard, as she continued to receive the respondent's newsletter.

By letter of 29 January 2022 in the ongoing proceedings before the Data Protection Authority, the respondent complied with the complainant's request for objection (which subsequently eliminated the alleged infringement of the non-accounted objection, in accordance with the first sentence of Paragraph 24(6) of the DSG) and, in summary, stated that it had been an accident and that she had now been removed from the newsletter mailing list.

The complainant did not dispute the receipt of this letter and stated that she had not received any further newsletters from the respondent.

Accordingly, the appeal procedure pursuant to Paragraph 24(6) of the DSG — as notified to the complainant by letter of 31 January 2022 — had to be closed informally (without a formal decision).

— 2 —

12. July 2022

For the Head of the Data Protection Authority:

[REDACTED]

GZ: D155.002
2022-0.279.505

Clerk: [REDACTED]

Data protection complaint (§ 24 DSG)

[REDACTED] (IMI-Nr.: A56ID 52843, 78540)

Via IMI

Subject: Final Decision; Amicable Settlement; Termination of the proceedings

On 14th of July 2018, [REDACTED] ("the complainant") lodged a complaint against [REDACTED] ("the controller") to the Bavarian Lander Office for Data Protection Supervision ("complaint-receiving SA"), claiming an infringement of the Right to erasure according to Art. 17 GDPR, because the controller failed to respond to the requests of the complainant from 9th of February 2018, 2nd of April 2018 and 25th of May 2018.

The controller complied by letter of 12th of August 2020 in the ongoing proceedings in front of the Austrian Data Protection Authority as the LSA to the complainant's request for erasure (which subsequently eliminated the alleged infringement of the non-executed deletion in accordance with the first sentence of Paragraph 24(6) of the national Data Protection Act (Datenschutzgesetz, DSG)).

The complainant did not dispute the access of this letter in the granted right to be heard and, despite two request from the complaint-receiving SA on 18th of June 2021 and 15th of July 2021, the complainant did not make any further submissions.

In summary, the controller subsequently removed the initial infringement by complying with the complainant's request in the letter from 12th of August 2020, and the complainant did not dispute this deletion despite the two above-mentioned requests. Therefore, the LSA assumes the satisfaction of the complainant and the LSA terminates the case by amicable settlement. For this reason, the complaint-receiving SA as well considers this complaint procedure to be settled.

Accordingly, the LSA terminates the complaint procedure informally - as communicated to the complainant via the complaint-receiving SA by letter from 17th of June 2021 - according to Paragraph 24 (6) DSG, because the initial infringement of Art. 17 GDPR was subsequently removed.

On behalf of the director of the Austrian Data Protection Authority



GZ: D155.062
2021-0.870.507

Clerk: [REDACTED]

Data Protection Complaint

[REDACTED] (A56ID 290715)

F I N A L D E C I S I O N

The Data Protection Authority decides on the data protection complaint of [REDACTED] (complainant) of 19 February 2021 against [REDACTED] (opponent) for an infringement of the right to secrecy (Austrian fundamental right to data protection) as follows:

1. The complaint is partially upheld and it is declared that the opponent has infringed the complainant's right to secrecy by processing his tax, income and bank account details, which the complainant submitted on 26 December 2020 and 27 January 2021, following their request, without any legal basis.

2. The opponent is requested to delete the data referred to in paragraph 1 within a period of four weeks.

3. The remainder of the complaint is dismissed as unfounded.

Legal bases: Article 4, Article 5(1)(c) and (e), Article 6(1)(a) and (e), Article 51(1), Article 57(1)(f), Article 58(2)(c) and Article 77(1) of Regulation (EU) 2016/679 (General Data Protection Regulation, 'the General Data Protection Regulation'). GDPR), Abl. No. L 119, 4.5.2016, p. 1; §§ 1, 18(1) and 24(1) and (5) of the Austrian Federal Act concerning the Protection of Personal Data (DSG), BGBl. I No 165/1999 as amended; § 1(1), § 2(1), § 5, § 6, § 7(1) and § 21(1)(1) and (6) of the Austrian Financial Market Money Laundering Act (FM-GwG), BGBl. I No 118/2016 as amended.

R E A S O N I N G

A. Arguments of the parties and course of proceedings:

1. The Data Protection Authority was notified of the complainant's complaint of 19 February 2021 by a notification from the Hungarian supervisory authority pursuant to Article 56 in conjunction with Art. 60 GDPR of 20 April 2021.

In summary, the complainant claimed that the opponent had requested from the complainant his personal income and tax return data. It has also requested access to his bank statement. In addition, the data was requested via e-mail, i.e. an insecure channel. The complainant has been a customer of the opponent since 2006 and has notified the opponent of his new address in Budapest two months ago. Upon request of the opponent, the complainant provided information on his tax return and his company registrations. Then the complainant was asked to translate the documents, which the complainant had done. However, the opponent refused to accept them and declared the complainant's credit card invalid due to failure to meet the "Know-your-Customer" (KYC) requirements. In all those years, the complainant had received almost EUR 100.000 from the opponent's credit card.

2. At the request of the Austrian data protection authority, the opponent stated in its submission from 30 August 2021, that as an Austrian bank, it was subject to the due diligence obligations for banks and that, pursuant to Paragraphs 5 et seq. of the the Austrian Financial Market Money Laundering Act (FM-GwG), it was required to obtain certain information from customers in order to prevent money laundering, terrorist financing and similar criminal offences. This includes getting an idea of your customers at regular intervals. This obligation stems from paragraph 7(6), sentence 1, of the FM-GwG. The complainant submitted those documents in Hungarian, so the opponent was legally obliged to insist on a certified translation.

On the basis of Article 6(1)(c) of the GDPR in conjunction with paragraph 7(6) sentence 1 FM-GwG, the opponent is entitled to obtain and process information about the data subjects. Moreover, the complainant was under no obligation to send the data in an unencrypted format. The complainant would also receive documents in password-protected form or by post.

3. By submission of 29 September 2021, submitted by the Hungarian supervisory authority on 2 October 2021, the complainant summarized that it was not clear from the KYC conditions that the complainant would have to provide employment details and income evidence on a regular basis. An official translation costs EUR 100 per page. The opponent did not give instructions to the complainant to upload sensitive documents securely. The opponent requested details by e-mail, which the complainant provided, and therefore the opponent did not act in accordance with the GDPR.

B. Subject of complaint

The subject of the complaint is whether the opponent has thereby violated the complainant in the (Austrian) fundamental right to data protection pursuant to § 1 para. 1 DSG respectively has infringed

Article 6 GDPR (lawfulness of processing) by requesting and processing his tax, income and account data received per e-mail.

C. Findings of the case

1. The complainant has been a customer of the opponent since 2006, which is a bank and credit institution from which he had a credit card.
2. The complainant moved from Vienna to Budapest in 2007 and informed the opponent of this.
3. In December 2020, the complainant informed that he had moved within Budapest.
4. Beginning with 18. December 2020, the opponent requested the complainant to provide information on his relationship with Austria and to provide several documents relating to his income and tax information. The complainant followed this request on 26 December 2020 and 27 January 2021, and submitted his income tax returns as well as a financial statement and a bank statement in Hungarian.
5. After the complainant was not willing to provide the Hungarian documents in a certified translation, the opponent dissolved the business relationship with the complainant.
6. The opponent did not ask the complainant to send the documents in question exclusively by e-mail.
7. In the course of the 14-year business relationship, the complainant has spent approximately EUR 100.000 via the opponent's credit card.

Appraisal of evidence: The findings are based as far as uncontested on the written statements of the parties. The findings on point 4 are based on the correspondence between the complainant and the opponent of 18, 19, 22, 26 and 28. December 2021 and 27 January 2022 submitted by the complainant. Points 2 and 6 are based on the complainant's statement, which was not disputed by the opponent.

D. Legal conclusions

Point 1 of the decision

Pursuant to Section 1(1) of the DSG, every person shall have the right to secrecy (fundamental right to data protection) of the personal data concerning that person, especially with regard to the respect for his or her private and family life, insofar as that person has an interest which deserves such protection. This means the protection of the data subject against the identification of his or her data and the protection against the disclosure of the data obtained about him. In purely conceptual terms, this process therefore presupposes the processing of personal data at the controller.

Pursuant to Section 1(2) of the DSG, restrictions on the right to secrecy are permitted only if the use of personal data takes place in the vital interest of the data subject or with his/her consent, in the case of overriding legitimate interests of another person or where a qualified legal basis exists.

The GDPR and in particular the principles enshrined therein must be taken into account in order to interpret the right to secrecy (cf. decision of the Austrian Data Protection Authority of 31 October 2018, GZ DSB-D123.076/0003-DSB/2018).

In the case of cross-border processing, such as here, there is in any case a violation of the fundamental right to data protection if Article 6 GDPR has been violated.

It must therefore be examined whether the processing of the proceedings can be based on one of the grounds of lawfulness referred to in Article 6 (1) of the GDPR.

Regarding the consent:

In Article 4 (11) GDPR, consent is defined as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

According to Art. 7 (4) GDPR and taking into account Art. 4 (11) and recital 43 GDPR, consent must be voluntary and must not be linked to the performance of a contract, although this consent is not necessary for the performance of this contract. Consent is involuntary if a disadvantage is to be expected if the consent is not given (cf. the decision of the Austrian Data Protection Authority of 16 April 2019, GZ DSB-D213.679/0003-DSB/2018).

In the present case, the question arises whether the complainant has freely given consent to the processing of his personal data in question or whether it has been valid and complies with the requirements laid down in the GDPR.

The complainant made it clear in his submission that he did not voluntarily consent to the processing of his transmitted data, as he would have expected a disadvantage if his income and financial data were not transmitted.

On vital interests:

In any event, the use of the data in question is not in the vital interest of the complainant.

The legal basis:

The opponent claimed that it was obliged to review its customers under the FM-GwG.

According to Art. 6(1)(c) GDPR, processing is lawful if it is necessary to fulfil a legal obligation to which the controller is subject.

Applicable legislation of the FM-GwG:

Paragraph 5 of the FM-GwG, together with its heading, reads as follows:

Application of due diligence obligations

§ 5. The obliged entities shall apply due diligence obligations towards customers in accordance with § 6 in the following cases:

1. when establishing a business relationship;

Savings deposit transactions pursuant to Section 31(1) of the BWG and transactions pursuant to Section 12 of the Depot Act shall always be regarded as a business relationship;

2. in the case of all transactions not falling within the scope of a business relationship (occasional transactions),

a) the amount of which amounts to at least EUR 15 000 or euro equivalent, irrespective of whether the transaction is made in a single operation or in several transactions between which a link is manifestly present; or

B) which are transfers of funds within the meaning of Article 3(9) of Regulation (EU) 2015/847 of more than EUR 1 000;

if the amount is not known in the cases referred to in point (a) before the commencement of the transaction, the due diligence obligations shall be applied as soon as the amount is known and it is established that it is at least EUR 15 000 or equivalent of euro;

3. for each deposit on savings deposits and at each disbursement of savings deposits, where the amount to be deposited or withdrawn is at least EUR 15 000 or equivalent;

4. if there is a suspicion or reasonable reason to believe that the customer belongs to a terrorist organisation (Section 278b StGB) or that the customer is objectively involved in transactions that serve the money laundering (Section 165 of the Criminal Code — including assets that result from a criminal act of the offender himself) or terrorist financing (Section 278d StGB);

5. in case of doubt as to the authenticity or adequacy of previously received customer identification data.

Paragraph 6(1) and (2) of the FM-GwG, together with the heading, read as follows:

Scope of due diligence obligations

§ 6. (1) The customer's due diligence obligations include:

1. Establishing the customer's identity and verifying identity on the basis of documents, data or information originating from a credible and independent source, including electronic means for identification and relevant trust services in accordance with Regulation (EU) No 910/2014 and other secure remote or electronic identification procedures in accordance with paragraph 4;

2. Establish the identity of the beneficial owner and take appropriate measures to verify his identity, so that obliged entities are convinced of knowing who the beneficial owner is; in the case of legal entities, trusts, companies, foundations and similar legal arrangements, appropriate measures are taken to understand the client's ownership and control structure. Where the identified beneficial owner is a member of the top management level pursuant to Section 2(1)(b) of the WiEReG, obliged entities shall take the appropriate measures necessary to verify the identity of the natural persons belonging to the top management level and shall keep records of the measures taken and of any difficulties encountered during the review operation. An appropriate measure is access to the register of beneficial owners in accordance with § 11 of the WiEReG;

3. Evaluation and collection of information on the purpose and nature of the business relationship;

4. Obtaining and verifying information on the origin of the funds used; such information may include, inter alia, the professional or business activity, income or results of business or the general financial situation of the client and its beneficial owners;

5. Identification and verification of the identity of the trustee and the trustee in accordance with paragraph 3;

6. continuous monitoring of the business relationship, including a review of transactions carried out in the course of the business relationship, in order to ensure that they are consistent with the obliged entities' knowledge of the customer, its business activities and its risk profile, including, where necessary, the origin of the funds;

7. periodically verify the existence of all information, data and documents required by this Federal Act, as well as updating this information, data and documents.

[...]

Paragraph 7(6) of the FM-GwG, together with its heading, reads as follows:

Date of application of due diligence obligations

§ 7. (1) The determination and verification of the identity of the customer, the beneficial owner, the trustee and the trustee (Section 6(1)(1), (2) and (5)) and the collection and verification of information about the purpose and the intended nature of the business relationship and the origin of the funds used (Section 6(1)(3) and (4)) must be made before establishing a business relationship and before carrying out an occasional transaction. The determination and verification of the identity of a natural person authorised to represent (Section 6(1) final part) must be carried out if the latter relies on his or her power of representation. At the beginning of a new business relationship with a legal entity pursuant to § 1WiEReG, the obliged entities must obtain an extract from the register of beneficial owners pursuant to § 9 or § 10 of the WiEReG as proof of the registration of the beneficial owners. At the beginning of a new business relationship with a company, trust, foundation, legal person comparable to a foundation, or with a similar trust-like legal arrangement established in another Member State or in a third country comparable to a legal entity within the meaning of Paragraph 1 of the WiEReG, obliged entities must obtain proof of registration or extract, provided that its beneficial owner must be registered in a register corresponding to the requirements of Articles 30 or 31 of Directive (EU) 2015/849.

[...]

(6) The obliged entities must apply the customer due diligence obligations not only to all new customers, but also to the existing clientele on a risk-based basis at an appropriate time. This is particularly the case where relevant circumstances change in the case of a customer, or where the obliged entity is legally obliged to contact the customer during the relevant calendar year to verify any relevant information about the beneficial owner or owners, or where the obliged entity is required to do so in accordance with Council Directive 2011/16/EU.

Paragraph 21(1)(1) and (6) of the FM-GwG, together with its heading, reads as follows (*emphasis added by the Data Protection Authority*):

Storage obligations and data protection

§ 21. (1) The obliged entities shall keep:

1. Copies of the documents and information received that are necessary for the fulfilment of customer due diligence obligations, including electronic means for identification and relevant trust services in accordance with Regulation (EU) No 910/2014, as well as other secure means of identification remotely or electronically in accordance with § 6(4), for a period of ten years after the end of the business relationship with the customer or after the date of an occasional transaction;

[...]

(6) The processing of personal data on the basis of this Federal Act, for the purpose of preventing money laundering and terrorist financing, is to be regarded as a matter of public interest in accordance with Regulation (EU) 2016/679. The safeguarding of public interests pursuant to Article 23(1) of Regulation (EU) 2016/679 may exist if the refusal to provide information (Section 20(1)) is necessary for the secrecy of transactions for the purpose of exercising Section 16 and Section 17 in order to:

1. enable the obliged entity or the FMA to properly perform his or her duties for the purposes of this Federal Act; or
2. not to impede administrative or judicial investigations, analyses, investigations or proceedings for the purposes of this Federal Act and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.

On the matter:

As a credit and financial institution pursuant to Paragraph 1(1) of the FM-GwG, the opponent is obliged to comply with the FM-GwG and acts as a credit institution within the meaning of Paragraph 1(1) of the BWG. As such, the opponent is subject to the due diligence obligations under FM-GwG and in accordance with the BWG.

In general, it should be noted that the FM-GwG aims to prevent money laundering and terrorist financing and therefore imposes certain due diligence obligations on credit (banking) institutions.

The opponent's statutory duty of care arises from Paragraph 6(1)(1) of the FM-GwG and includes the 'determination of the customer's identity and verification of identity on the basis of documents, data or information originating from a credible and independent source'.

Paragraph 6(1)(6) of the FM-GwG is one of the key standards in the assessment of legal obligations for the prevention of money laundering and terrorist financing. Accordingly, customer due diligence shall include the continuous monitoring of the business relationship, including a review of transactions carried out in the course of the business relationship, in order to ensure that they are consistent with the knowledge of the obliged entities about the customer, its business activities and its risk profile, including, where necessary, the origin of the funds.

For example, Paragraph 5(1) of the FM-GwG regulates an obligation on the opponent to apply the due diligence obligations laid down in Paragraph 6 of the FM-GwG in the event of establishing a permanent business relationship, whereby this obligation arises according to the materials already before the establishment of the business relationship. The application of the due diligence obligations should therefore already be concluded with the conclusion of the contract (see *Hörtner in Hörtner/Trautmann*, Praxishandbuch FM-GwG (2020) § 5, paragraph 2 (as at 1.10.2020, rdb.at)).

At the time of the transfer of the data, the complainant was already a long-standing customer of the opponent, who regularly used the opponent's credit card, therefore the scope of Paragraph 5(1) FM-GwG cannot be considered.

Although the complainant has argued that he spent a total of EUR 100.000 on the credit card during the 14-year business relationship, however, not every transaction constitutes a transaction in favour of the above-mentioned frowned upon purposes.

Nor did the opponent submit that those transactions were occasional transactions or transactions outside a business relationship with an amount exceeding EUR 15.000 or transfers of funds within the meaning of Article 3(9) of Regulation (EU) 2015/847 of more than EUR 1.000. There are no other indications for the opposite. Thus, the scope of Paragraph 5(2) of the FM-GwG is also excluded.

The scope of Paragraph 5(3) of the FM-GwG is also excluded, since there are also no indications here.

Pursuant to Section 5(4) FM-GwG, the obliged party must already apply due diligence measures in the event of suspicion of money laundering or terrorist financing. However, there are no indications to the

complainant regarding money laundering or terrorist financing, nor have they been put forward by the opponent.

Pursuant to § 7(6) FM-GwG, the opponent has to apply the customer due diligence obligations not only to all new customers, but also to the existing customers at an appropriate time on a risk-based basis. This is especially the case if significant circumstances change with a customer.

The complainant has been living in Budapest since 2007, therefore his place of residence has not changed.

The opponent did not put forward any reason why it had to apply due diligence obligations or what relevant circumstances have changed to the complainant that the opponent had to assume a risk of money laundering or terrorist financing.

In this context, reference should also be made to the principle of data minimisation in accordance with Article 5(1)(c) of the GDPR, according to which the processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In addition, both the circular of Austrian Financial Market Authority (FMA) 09/2018 and the case law of the Austrian Federal Administrative Court (BVwG) speak of risk-oriented and appropriate (adequate) measures:

"Client-level risk assessment is the basis for a risk-oriented and appropriate application of due diligence. Obliged persons must be able to demonstrate the adequacy of the measures implemented by the FMA" (cf. circular FMA 09/2018, p. 10).

'The risk assessment procedure installed during the period in XXXX, which made it possible to identify business relationships established by way of distance business which, by their very nature, constitute an increased risk and are also considered to be 'higher risk' under the XXXX internal working instructions, was not appropriate and appropriate in the actual risk assessment of long-distance customers' (cf. BVwG, W210 2000428-1, 19.09.2014).

With regard to the customer with the number XXXX ("XXXX"), XXXX has since 01.09.2010 failed to take risk-based and appropriate measures to verify the identity of the beneficial owner of the customer, so that he is convinced of who the beneficial owner of that customer was (cf. BVwG, W210 2000428-1, 19.09.2014).

There is no evidence from the findings established and from the arguments of the parties that the complainant has placed a conspicuous conduct or conspicuous transaction or that he was at all assessed as a risk by the opponent. Therefore there are no indications or reasonable grounds to believe that the complainant belongs to a terrorist organisation within the meaning of Paragraph 278b of the Austrian penal code (StGB) or that he is objectively involved in transactions that serve the money laundering pursuant to Section 165 of the StGB — including elements of assets resulting from a criminal act of the offender himself — or the financing of terrorism pursuant to § 278d StGB.

Regarding the legitimate interests:

The opponent has also not raised any legitimate interests that outweigh an infringement of the right to secrecy.

Result:

The Data Protection Authority therefore concludes that due to the examination of the requirements of the FM-GwG, the application of due diligence obligations to the relevant data processing (income and tax information of the complainant) was not applicable. Therefore, the processing in question of the complainant's personal data took place without the existence of a qualified legal basis.

The decision was therefore appropriate.

Point 2:

Since the conditions for the processing of the data subject to the procedure were not met, they were processed unlawfully from the beginning, which is why they must be deleted in accordance with Article 17(1)(d) of the GDPR.

The data protection authority therefore makes use of its power in accordance with Article 58(2)(g) of the GDPR (for the admissibility of an official order see the decision of the Austrian Federal Administrative Court of 4 June 2019, GZ W214 2213623-1).

Point 3:

Insofar as the complainant complains that the opponent has violated his privacy, since his financial data had been requested via an unsecured channel (by e-mail), no specific violation of rights was identified, especially since the GDPR cannot be derived from a legal claim for compliance with certain data security measures (decision of the Austrian Federal Administrative Court of 9. December 2021, GZ W214 2225733-1).

In addition, there are no indications that these emails have been disclosed to unauthorized third parties.

It was therefore appropriate to decide in accordance with the judgment.

23. Juni 2022

Für die Leiterin der Datenschutzbehörde:



GZ: D155.024
2022-0.620.529

Sachbearbeiter [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
zH «zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint

[REDACTED] (IMI Nr.: A56ID 124562)

Subject: Final Decision:

The complainant [REDACTED] raised on 16. December 2019 against [REDACTED] (controller) a complaint and claimed that the controller had not responded to its request of 7 November 2019 (Art. 15 GDPR „Right of access by the data subject“).

The controller replied by letter of 11. December 2020 in the ongoing proceedings before the Data Protection Authority, to the complainant's right of access by the complainant (which subsequently eliminated the alleged infringement of the non-existence of the right of access). Thus, an amicable agreement could be reached between the complainant and the respondent.

The complainant did not dispute the receipt of this letter in the parties granted to it and, despite a request to that effect, did not submit any further submissions. A corresponding forwarding report is attached to the act and there is no error message from an e-mail server.

Accordingly, the appeal proceedings had to be closed informally (without notice).

****Genehmigungsdatum****

Für die Leiterin der Datenschutzbehörde:

****Genehmiger(in)****

GZ: D155.014
2022-0.751.089

Clerk: [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (§ 24 DSG)
[REDACTED]

by RSb/letter/e-mail «emailadresse»

Subject: Communication; Cessation of the procedure

In his complaint of 7 May 2019 addressed to the Land Commissioner for Data Protection Lower Saxony (LfD), the complainant, [REDACTED], claimed that he had been infringed in his right to information by the respondent, [REDACTED].

By letter dated 19 February 2020, the respondent complied with the complainant's request for information, which subsequently eliminated the alleged infringement.

The complainant did not dispute the receipt of the respondent's letter within the scope of the party's association and did not submit any further submissions despite a request to that effect.

The appeal procedure was therefore terminated.

Genehmigungsdatum

Für die Leiterin der Datenschutzbehörde:

o.b. ***Genehmiger(in)***

GZ: D155.070
2022-0.803.857

Clerk: [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
zH «zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (§ 24 DSG)

[REDACTED] (IMI-Nr.: A56ID 329311, 329930, A60DD 446974)

by RSb/letter/email «emailadresse»

Subject: Communication; Termination of proceedings, Final Decision

The complainant [REDACTED] lodged a complaint with the Swedish Data Protection Supervisory Authority in October 2021 against [REDACTED] (respondent) against the Data Protection Authority claiming an infringement of the right to object by failing to respond to its request in this regard.

By letter of 21 October 2021, the respondent responded in the ongoing proceedings before the data protection authority to the complainant's request for an objection (which subsequently eliminated the alleged infringement of the objection which had not been taken into account, in accordance with the first sentence of Paragraph 24(6) of the DSG).

The complainant did not dispute the access of this letter in the party hearing granted to it and, despite the request to that effect, did not make any further submissions. A corresponding forwarding report is attached to the act and there is no error message of an email server.

Accordingly, as communicated to the complainant by letter from the Data Protection Authority of 22 October 2021, the appeal procedure pursuant to Section 24(6) of the DSG was to be terminated informally (without decision).

11. November 2022

Für die Leiterin der Datenschutzbehörde:

Genehmiger(in)

GZ: D155.038
2022-0.909.487

Sachbearbeiter [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
zH «zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (Art. 15 GDPR)
[REDACTED] (IMI-Nr.: A61ID 167383)

Subject: Final Decision:

The complainant [REDACTED] lodged a complaint against [REDACTED] (respondent) to the Data Protection Authority on 23 July 2020 (received by the Austrian Data Protection Authority on 30 November 2020) against [REDACTED] (respondent) to the Data Protection Authority, alleging a breach of the right to information by failing to respond to his request of 29 March 2020.

By letter of 10 February 2021, the Respondent complied with the complainant's request for information in the ongoing proceedings before the Data Protection Authority (which subsequently corrected the alleged infringement of the failure to delete it). Thus, an amicable agreement could be reached between the complainant and the respondent.

The complainant did not dispute the receipt of this letter in the parties granted to it and, despite a request to that effect, did not submit any further submissions. A corresponding forwarding report is attached to the act and there is no error message from an e-mail server.

After the controller had complied with the right to information in accordance with Art. 15 GDPR during the ongoing proceedings, this could be settled as part of an amicable agreement.

Genehmigungsdatum

Für die Leiterin der Datenschutzbehörde:

I.A. **Genehmiger(in)**

GZ: D155.072
2022-0.447.220

Desk Officer: [REDACTED]

Data protection complaint (§ 24 DSG)
[REDACTED] (A56ID 329823)

Via IMI

Subject: Draft Decision; amicable settlement

On 3 June 2021, Complainant [REDACTED] filed a complaint against [REDACTED] (respondent) to the Data Protection Authority, alleging an infringement of the right to erasure.

The respondent replied by letter of 6 December 2021, in the ongoing proceedings before the Data Protection Authority, as the lead supervisory authority, informs that the desired deletion of the account was carried out and that e-mails can no longer be sent (which subsequently eliminated the alleged infringement in accordance with § 24(6) first sentence of the DSG).

The complainant did not dispute the access to this letter in the party belonging to it granted by the German Supervisory Authority Baden-Württemberg and did not submit any further submissions.

Accordingly, the complaint procedure pursuant to § 24(6) DSG — as the complainant via the German Supervisory Authority Baden-Württemberg by letter of 7 December 2021 — had to be closed informally (without official ruling).

20.12.2022

On behalf of the Head of the Austrian Data Protection Authority:

[REDACTED]

GZ: D155.064
2022-0.447.282

Desk officer: [REDACTED]

Data protection complaint (§ 24 DSG)
[REDACTED] (A56ID 316623)

Via IMI

Subject: Draft Decision; amicable settlement

On 11 June 2021, complainant [REDACTED] filed a complaint against [REDACTED] (respondent), now [REDACTED] to the Data Protection Authority, alleging an infringement of the right to erasure.

By letter of 10 November 2021, the Respondent informed in the ongoing proceedings before the Data Protection Authority, as the lead supervisory authority, that the desired deletion was carried out (which subsequently eliminated the alleged infringement in accordance with § 24(6) first sentence DSG).

The complainant did not dispute the access of this letter in the party belonging to it granted by the North Rhine-Westphalia State Commissioner for Data Protection and Freedom of Information and did not submit any further submissions.

Accordingly, the appeal procedure pursuant to § 24(6) of the DSG — as notified to the complainant via the North Rhine-Westphalia State Commissioner for Data Protection and Freedom of Information by letter of 11 November 2021 — had to be closed informally (without official ruling).

20.12.2022

On behalf of the Head of the Austrian Data Protection Authority

[REDACTED]

GZ: D155.068
2023-0.051.671

Sachbearbeiter [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (right to information)

[REDACTED] (IMI-Nr.: A56ID 319178)

Subject: 'Sui generis', Final Decision:

On 17 November 2019 (received by the Austrian Data Protection Authority on 25 August 2021), the complainant [REDACTED] lodged a complaint against [REDACTED] (respondent) to the Data Protection Authority against [REDACTED] (respondent) to the Data Protection Authority, alleging an infringement of the right to information pursuant to Article 15 GDPR by failing to respond to his request for information of 27 August 2019.

By letter of 29 September 2021, the Respondent complied with the complainant's request for information in the ongoing proceedings before the Data Protection Authority (which subsequently eliminated the alleged infringement of the non-existent information). Thus, an amicable agreement could be reached between the complainant and the respondent.

The complainant did not dispute the receipt of this letter in the parties granted to it and, despite a request to that effect, did not submit any further submissions.

Accordingly, the appeal proceedings had to be closed informally (without notice).

Genehmigungsdatum

Für die Leiterin der Datenschutzbehörde:

I.A. **Genehmiger(in)**

GZ: DSB-D155.004/0005-DSB/2019

Clerk: [REDACTED]

[REDACTED]
Subject: Closure of the proceedings due to withdrawal of the complaint, Final decision

1. In its complaint of 5 February 2019 against the respondent, [REDACTED], the complainant, [REDACTED], essentially submitted that the respondent had carried out a credit assessment at [REDACTED] in breach of Article 6 of the DSGVO.

2. In its statement of 2 July 2019, the respondent stated that the inquiry at [REDACTED] had not concerned the complainant but another customer of the same name.

3. On 1 August 2019, after receiving the letter of settlement in which it was mentioned based on the respondent's comments that she could withdraw her complaint, the complainant announced by telephone to the supervisory authority concerned that the case could be concluded.

The Austrian data protection authority therefore announces that the complaint proceedings will be closed due to the withdrawal of the complaint.

12. January 2023

On behalf of the head of the data protection authority
[REDACTED]

Ref. No.: D130.087
2020-0.778.655

clerk: [REDACTED]

Data protection complaint (erasure)

[REDACTED] (IMI-Nr.: A56ID 48938, A61VM 90233, A60DD 164846)

Decision of the data protection authority

D E C I S I O N

S P E E C H

The data protection authority decides on the data protection complaint of [REDACTED] (complainant) of 7.8.2018 against [REDACTED] (respondent) for violation of the right to erasure as follows:

- The complaint is dismissed.

Legal basis: Art 4 Z 23 lit. b, Art. 51 para. 1, Art. 56 Para. 1, 57 para. 1 lit. f, Art. 60 para. 8, Art. 77 para. 1 and Art. 85 of the Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), OJ No. L 119, 4.5.2016, p. 1; §§ 18 para. 1 and 24 para. 1 and para. 5 of the Data Protection Act (DSG), BGBl. I No. 165/1999 as amended.

J U S T I F I C A T I O N

A. Arguments of the parties and course of proceedings

1. In her complaint submitted to the Austrian data protection authority, the complainant, who resides in Austria, essentially alleged that personal data relating to her was visible on the website "[REDACTED]" operated by the complainant. She had attended a postgraduate course in Sweden from 2012 to 2013 and had a Swedish cell phone contract at the time. She suspected that the data published on the website had reached the complainant via this cell phone contract. She had not consented to any publication.

She had sent a request for deletion to the respondent by e-mail on July 18, 2018. However, the respondent had not responded to it.

2. Since the case involved a cross-border issue, the Austrian data protection authority placed the case in the "Internal Market Information (IMI) System" used under the consistency mechanism to handle the cross-border procedure under the provisions of the GDPR. It turned out that the main establishment of the respondent is [REDACTED], located at [REDACTED].

Accordingly, pursuant to Art. 56 Para. 1 GDPR, the Swedish supervisory authority is the lead supervisory authority in these proceedings. This fact was communicated to the complainant by letter dated 13.12.2018, GZ DSB-D130.087/0004-DSB/2018.

3. The Swedish supervisory authority submitted a draft decision on 20.11.2020 pursuant to Art. 60 para. 3 GDPR. This essentially states that so-called publication certificates ("utgivningsbevis") can be applied for websites under Swedish law. The Swedish Press and Broadcasting Authority is responsible for issuing the publication certificates. This meant that data protection laws were not applicable to information published on such websites. The website operated by the respondent had obtained such a publication certificate. The GDPR allows Member States to make exceptions to the rules if this is necessary to safeguard the right to freedom of expression and information (Art. 85 GDPR). The Swedish Constitution (Freedom of the Press Act) allows such information to be published. There is an exceptional provision pursuant to Art. 85 GDPR, so that the GDPR is not applicable. There is therefore no competence of the Swedish supervisory authority.

B. Subject-matter of the complaint

The subject matter of the complaint is the question whether the respondent has thereby violated the complainant's right to erasure pursuant to Art. 17 GDPR by not complying with the request for erasure.

C. Establishment of the facts

The data protection authority bases its decision on the facts of the case as set forth in item A. and documented in the file.

D. From a legal point of view, it follows:

The data processing subject of the complaint is cross-border data processing within the meaning of Article 4(23)(b) of the GDPR, as the complainant is resident in Austria, but the controller (respondent)

is established in Sweden. The lead supervisory authority was therefore the Swedish supervisory authority pursuant to Art. 56 para. 1 GDPR.

In the course of the proceedings, the lead Swedish supervisory authority came to the conclusion that the complaint concerns a matter that is not subject to the scope of application of the GDPR or the competence of the Swedish supervisory authority. Sweden has in fact - similar to Austria in § 9 para. 1 of the Austrian Data Protection Act - made use of the "opening clause" contained in Art. 85 GDPR and established exceptions for such data processing operations in order to safeguard the right to freedom of expression and information.

The Swedish supervisory authority notified the Austrian data protection authority of this circumstance pursuant to Art. 60 para. 3 GDPR in its decision of 20.11.2020. There was no occasion for a relevant and reasoned objection.

If a complaint is rejected or dismissed, the supervisory authority to which the complaint was submitted shall adopt the decision and notify the complainant and inform the controller, in accordance with Art. 60 para. 8 GDPR. This is the case here. For this reason, the decision in question is issued by the Austrian data protection authority.

Therefore, the decision had to be made in accordance with the ruling.

LEGAL NOTICE

An appeal against this decision may be lodged in writing with the Federal Administrative Court within four weeks of notification. The complaint must be lodged with the data protection authority and must be

- the name of the contested decision (GZ, subject)
- the name of the authority being prosecuted,
- the grounds on which the allegation of illegality is based,
- desire and
- the information necessary to assess whether the complaint has been lodged in good time, must be included.

The data protection authority may within two months either amend its decision by means of a preliminary decision on the complaint or submit the complaint with the files of the proceedings to the Federal Administrative Court.

The appeal against this decision is subject to a fee. The fixed fee for a corresponding submission including enclosures is 30 euros. The fee is to be paid into the account of the tax office for fees,

transaction taxes and gambling (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW), whereby the respective appeal procedure (business number of the notice) is to be stated as the purpose of payment on the payment order.

In the case of electronic transfer of the appeal fee with the "tax office payment", the tax office for fees, transaction taxes and gambling (IBAN as before) must be stated or selected as the recipient. In addition, the tax number/tax account number 109999102, the tax type "EEE - complaint fee", the date of the notice as the period and the amount must be stated.

The payment of the fee must be proven to the data protection authority when the complaint is lodged by means of a original payment receipt confirmed by a postal office or a credit institution, which must be attached to the submission. If the fee is not paid or not paid in full, a report is sent to the competent tax office.

A timely filed and admissible appeal to the Federal Administrative Court has suspensive effect. The suspensive effect may have been excluded in the ruling of the decision or may have been excluded by a separate decision.

January 7, 2021

For the head of the data protection authority:

[REDACTED]

GZ:D130.340
2021-0.049.824

Clerk: [REDACTED]

Data protection complaint
[REDACTED]

D E C I S I O N

S P E E C H

The data protection authority decides on the data protection complaint of [REDACTED] (complainant) dated 12 September 2019 against [REDACTED] (respondent) for violation of the right to erasure as follows:

- The complaint is dismissed.

Legal basis: Art 4 Z 23 lit. b, Art. 51 para. 1, Art. 56 Para. 1, 57 para. 1 lit. f, Art. 60 para. 8, Art. 77 para. 1 and Art. 85 of the Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), OJ No. L 119, 4.5.2016, p. 1; §§ 18 para. 1 and 24 para. 1 and para. 5 of the Data Protection Act (DSG), BGBI. I No. 165/1999 as amended.

J U S T I F I C A T I O N

A. Arguments of the parties and course of proceedings

1. In her complaint sent to the Austrian data protection authority on 12 September 2019, the complainant who resides in Austria, essentially alleged that the website [REDACTED] shows her personal data. Obviously, her Swedish mobile phone provider at the time had passed on her data. On 13 June 2019, she submitted a request for deletion to the respondent by e-mail. However, the respondent did not respond.
2. Since the case involved a cross-border issue, the Austrian data protection authority placed the case in the "Internal Market Information (IMI) System" used under the consistency mechanism to handle the cross-border procedure under the provisions of the GDPR. It turned out that the main establishment of the respondent is in Sweden. Accordingly, pursuant to Art. 56 Para. 1 GDPR, the Swedish supervisory

authority is the lead supervisory authority in these proceedings. This fact was communicated to the complaint by letter dated 23 January 2020.

3. The Swedish supervisory authority submitted a draft decision on 13 November 2020 in accordance with Art.60 (3) GDPR. This essentially states that so-called publication certificates ("utgivningsbevis") can be applied for websites under Swedish law. The Swedish Press and Broadcasting Authority is responsible for issuing the publication certificates. This meant that data protection laws were not applicable to information published on such websites. The website operated by the respondent had obtained such a publication certificate. The GDPR allows Member States to make exceptions to the rules if this is necessary to safeguard the right to freedom of expression and information (Art. 85 GDPR). The Swedish Constitution (Freedom of the Press Act) allows such information to be published. There is an exceptional provision pursuant to Art. 85 GDPR, so that the GDPR is not applicable. There is therefore no competence of the Swedish supervisory authority

B. Subject-matter of the complaint

The subject matter of the complaint is the question whether the respondent has thereby violated the complainant's right to erasure pursuant to Art. 17 GDPR by not complying with the request for erasure.

C. Establishment of the facts

The data protection authority bases its decision on the facts of the case as set forth in item A. and documented in the file.

D. From a legal point of view, it follows:

The data processing subject of the complaint is cross-border data processing within the meaning of Article 4(23)(b) of the GDPR, as the complainant is resident in Austria, but the controller (respondent) is established in Sweden. The lead supervisory authority was therefore the Swedish supervisory authority pursuant to Art. 56 para. 1 GDPR.

In the course of the proceedings, the lead Swedish supervisory authority came to the conclusion that the complaint concerns a matter that is not subject to the scope of application of the GDPR or the competence of the Swedish supervisory authority. Sweden has in fact - similar to Austria in § 9 para. 1 of the Austrian Data Protection Act - made use of the "opening clause" contained in Art. 85 GDPR and established exceptions for such data processing operations in order to safeguard the right to freedom of expression and information.

The Swedish supervisory authority notified the Austrian data protection authority of this circumstance pursuant to Art. 60 para. 3 GDPR in its decision of 13. November 2020. There was no occasion for a relevant and reasoned objection.

If a complaint is rejected or dismissed, the supervisory authority to which the complaint was submitted shall adopt the decision and notify the complainant and inform the controller, in accordance with Art. 60 para. 8 GDPR. This is the case here. For this reason, the decision in question is issued by the Austrian data protection authority.

Therefore, the decision had to be made in accordance with the ruling.

LEGAL NOTICE

An appeal against this decision may be lodged in writing with the Federal Administrative Court within four weeks of notification. The complaint must be lodged with the data protection authority and must be

- the name of the contested decision (GZ, subject)

- the name of the authority being prosecuted,

- the grounds on which the allegation of illegality is based,

- desire and

- the information necessary to assess whether the complaint has been lodged in good time, must be included.

The data protection authority may within two months either amend its decision by means of a preliminary decision on the complaint or submit the complaint with the files of the proceedings to the Federal Administrative Court. The appeal against this decision is subject to a fee. The fixed fee for a corresponding submission including enclosures is 30 euros. The fee is to be paid into the account of the tax office for fees, transaction taxes and gambling (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW), whereby the respective appeal procedure (business number of the notice) is to be stated as the purpose of payment on the payment order.

In the case of electronic transfer of the appeal fee with the "tax office payment", the tax office for fees, transaction taxes and gambling (IBAN as before) must be stated or selected as the recipient. In addition, the tax number/tax account number 109999102, the tax type "EEE - complaint fee", the date of the notice as the period and the amount must be stated.

The payment of the fee must be proven to the data protection authority when the complaint is lodged by means of a original payment receipt confirmed by a postal office or a credit institution, which must

be attached to the submission. If the fee is not paid or not paid in full, a report is sent to the competent tax office.

A timely filed and admissible appeal to the Federal Administrative Court has suspensive effect. The suspensive effect may have been excluded in the ruling of the decision or may have been excluded by a separate decision

January 22, 2021

For the head of the data protection authority:





Barichgasse 40-42
A-1030 Vienna
Tel.: +43-1-52152 302581

E-Mail: dsb@dsb.gv.at

GZ: D130.075
2021-0.011.307

clerk: [REDACTED].

[REDACTED]
Data protection complaint (§ 24 DSG - Austrian Data Protection Act)

[REDACTED] (IMI-Nr.: A56 ID 48903)

via E-Mail: [REDACTED]

Subject: Notification; termination of the proceedings

The complainant announced by telephone on 8.1.2021 that he was withdrawing his complaint pursuant to Section 13 (7) AVG (General Administrative Procedure Act).

The procedure was therefore to be discontinued informally (without a decision) and the data protection authority hereby brings this to your attention.

8. January 2021

For the head of the data protection authority:

[REDACTED]



Republik Österreich
Datenschutz
behörde

Barichgasse 40-42
A-1030 Vienna
Tel.: +43-1-52152 302578

E-Mail: dsb@dsb.gv.at

Ref. No.: D130.087 2020-0.778.655

clerk: [REDACTED]

Data protection complaint (erasure)
[REDACTED]

(A56ID 48459, A60DD 164838)

Decision of the data protection authority

D E C I S I O N

S P E E C H

The Data Protection Authority decides on the data protection complaint of [REDACTED] (complainant) dated 08 June 2018 against [REDACTED] (opponent) for violation of the right to erasure as follows:

— The complaint is dismissed.

Legal basis: Art. 4 subpara 23 lit. b, Art. 51 para 1, Art. 56 para 1, 57 para 1 lit. f, Art. 60 para 8, Art. 77 para 1 and Art. 85 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter:GDPR), OJ L 119, 4.5.2016 p. 1; §§ 18 para 1 and 24 para 1 and para 5 of the Data Protection Act (DSG), Federal Law Gazette I No. 165/1999 idgF.

E X P L A N A T O R Y M E M O R A N D

A. Arguments of the parties and proceeding

1. In her complaint sent to the data protection authority, the complainant resident in Austria essentially argued that the respondent's website [REDACTED] showed personal data from her. She completed a postgraduate course in Sweden from 2012 to 2013 and had a Swedish mobile phone contract at the time. It was presumed that the data published on the website had reached the complainant via this mobile phone contract. It did not agree to any publication.

In June 2018, it submitted a request for deletion to the respondent by e-mail. However, the latter refused to delete it.

2. Since this is a cross-border matter, the data protection authority put the case in the "Internal Market Information (IMI) system", which is used in the context of the coherence procedure to handle the cross-border procedure in accordance with the provisions of the GDPR. It turned out that the respondent's main place of business is in Sweden.

According to Art. 56 (1) GDPR, the Swedish supervisory authority is the leading supervisory authority of this procedure. This circumstance was communicated to the appellant.

3. The Swedish supervisory authority considered itself responsible for the content handling and submitted a draft decision on 20 November 2020 in accordance with Art. 60(3) GDPR. This essentially shows that for websites under Swedish law, so-called "utgivningsbevis" can be applied for. The Swedish Press and Broadcasting Authority was responsible for issuing the publication certificates. This means that the data protection laws are not applicable to information published on such websites. The website operated by the respondent received such a publication certificate. The GDPR allows Member States to make exceptions to the regulations if this is necessary in order to safeguard the right to freedom of expression and information (Art. 85 GDPR). The Swedish Constitution (Press Freedom Act) allows such information to be published. There is a derogation according to Art. 85 GDPR. There was no competence of the Swedish supervisory authority.

B. Subject-matter of the complaint:

The subject-matter of the complaint is whether the Respondent has thereby infringed the complainant in its right to erasure in accordance with Art. 17 GDPR by failing to comply with the request for deletion.

C. Establishment of the facts:

The data protection authority shall base its decision on the facts set out in point A. and documented on time.

D. From a legal point of view, it follows:

The subject-matter data processing is a cross-border data processing in accordance with Art. 4 subpara 23 lit. b GDPR, since the complainant is domiciled in Austria, but the person responsible (opponent) is established in Sweden. The leading supervisory authority was therefore the Swedish supervisory authority in accordance with Art. 56 (1) GDPR.

In the course of the proceedings, the leading Swedish supervisory authority came to the conclusion that the complaint concerns a matter which is not subject to the scope of the GDPR or to the competence of the Swedish supervisory authority. Sweden has made use of the “opening clause” contained in Art. 85 GDPR, similar to Austria in § 9 para. 1 DSG, and has set exceptions for such data processing operations in order to safeguard the right to freedom of expression and information.

In its decision of 20 November 2020, the Swedish supervisory authority informed the Austrian data protection authority of this circumstance in accordance with Article 60(3) GDPR. There was no reason for a decisive and reasoned opposition.

If a complaint is rejected or rejected, the supervisory authority with which the complaint has been lodged shall issue the decision and notify the complainant to the complainant in accordance with Article 60(8) GDPR. It's the case here. For this reason, the present decision is taken by the Austrian Data Protection Authority.

It was therefore appropriate to decide.

L E G A L N O T I C E

A complaint to the Federal Administrative Court may be lodged against this decision in writing within four weeks of notification. The complaint must **be lodged with the data protection authority** and must:

- the name of the contested decision (GZ, subject)
- the designation of the authority concerned;
- the grounds on which the allegation of illegality is based,
- desire as well as
- the information necessary to assess whether the appeal has been lodged in time;

included.

The data protection authority has the option, either by means of a preliminary complaint decision, to amend **its** decision or to **submit the complaint with the files of the procedure** to the Federal Administrative Court.

The appeal against this communication is **subject to a fee**. The fixed fee for a corresponding input including supplements is **EUR 30**. The fee is due to the account of the Tax Office for Fees, Traffic Taxes and Gambling (IBAN:AT83 0100 0000 0550 4109, BIC:BUNDATWW) where the respective complaint procedure (the number of transactions of the communication) must be indicated on the payment order as intended for use.

In the case of electronic transfer of the appeal fee with the "financial payment", the tax office for fees, transport taxes and gambling (IBAN as before) shall be indicated or selected as the recipient. Furthermore, the tax number/tax account number 109999102, the type of tax "EEE complaint fee", the date of the decision as the period and the amount must be indicated.

The payment **of the fee** shall be **demonstrated** when the complaint is lodged with the **data protection authority** by means of an original payment document (original) confirmed by a post office or a credit institution. If the fee is not paid or not paid in full, a **notification shall be sent to the competent tax office**.

A timely and admissible appeal to the Federal Administrative Court has **suspensive effect**. The suspensive effect may have been excluded in the statement of the decision or may be excluded by an own decision.

February 10th, 2021

For the Head of the Data Protection Authority:



D E C I S I O N

S P E E C H

The data protection authority decides on the data protection complaint of [REDACTED] (complainant) of 10.4.2019 against [REDACTED] with registered office in Hamburg, Germany, (respondent) for violation of the right of access as follows:

- The complaint is dismissed.

Legal basis: Art. 4 Z 23 lit. b, Art. 15, Art. 51 para. 1, Art. 56 para. 1, 57 para. 1 lit. f, Art. 60 para. 8, Art. 77 para. 1 as well as Art. 85 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter: GDPR), OJ No. L 119, 4.5.2016 p. 1; §§ 18 para. 1 as well as 24 para. 1 and para. 5 of the Austrian Data Protection Act (DSG), Federal Law Gazette I No. 165/1999 as amended.

J U S T I F I C A T I O N

A. Arguments of the parties and course of the proceedings

1. By complaint dated 10.4.2019, as improved by submission dated 8.5.2019, the complainant alleged a violation of the right of access and, in summary, submitted that on 25.1.2019 and 26.1.2019, he had participated in a selection procedure for pilots conducted by the respondent. In the context of this procedure, the respondent had collected personal data from him. On 22.2.2019, he sent a request for information to the respondent by post. The letter was demonstrably taken over by an employee of the respondent on 25.2.2019. However, the respondent did not react to this request.
2. Since the case involved a cross-border issue, the data protection authority placed the case in the "Internal Market Information (IMI) System", which is used under the consistency mechanism to handle the cross-border procedure under the provisions of the GDPR. It turned out that the main office of the respondent in Hamburg is in Germany.

According to Article 56(1) of the GDPR, the Hamburg Commissioner for Data Protection and Freedom of Information was the lead supervisory authority in these proceedings. This fact was communicated to the complainant.

3. The Hamburg Commissioner for Data Protection and Freedom of Information considered himself responsible for dealing with the content and forwarded the complaint to the respondent.

4. In its opinion, the respondent submitted that it had provided the complainant with information by e-mail of 21.3.2019, namely that it had deleted all of the complainant's personal data due to the fact that the complainant had not passed the selection procedure.

5. The respondent's statement was subsequently sent to the complainant by letter of the data protection authority dated 28.11.2019, ref. DSB-D130.254/0003-DSB/2019, together with a request to comment on whether the complainant had received the respondent's email of 21.3.2019.

6. In his statement of 12 December 2019, the complainant essentially argued that he had definitely not received the respondent's e-mail of 21 March 2019. It was not even clear from the enclosure sent to which e-mail address the e-mail was supposed to have been sent.

7. The complainant's opinion was forwarded to the lead supervisory authority. The supervisory authority subsequently submitted a draft decision pursuant to Article 60(3) of the GDPR. The draft decision stated that it could not be proven whether the complainant had actually received the respondent's e-mail. Although the complainant's denial of receipt cast doubt on the proper provision of information, the complainant had at least received the negative information provided in the course of the proceedings. Thus, the respondent had fulfilled its accountability obligation under Article 56(2) of the GDPR. The law did not set high requirements for the obligations of the controller and it was therefore up to the supervisory authority to prove a violation. There were no possibilities for this, even after consultation with IT employees. In the event that such incidents were to occur more frequently at the respondent, appropriate measures would be taken.

B. Subject of the complaint

The subject matter of the complaint is the question whether the respondent has violated the complainant's right of access pursuant to Art. 15 GDPR.

C. Findings of fact

The data protection authority bases its decision on the facts of the case as set out in point A. and documented in the file.

D. In legal terms, it follows that:

The data processing subject of the complaint is a cross-border data processing within the meaning of Art. 4(23)(b) of the GDPR, as the complainant is resident in Austria, but the controller (respondent) is established in Hamburg, Germany. The Hamburg Commissioner for Data Protection and Freedom of Information was therefore the lead supervisory authority pursuant to Art. 56(1) of the GDPR.

In the course of the proceedings, the lead supervisory authority came to the conclusion that although it was not verifiable whether the complainant had received the requested information by e-mail of

21.3.2019, the complainant had received the information in the course of the proceedings (via the Austrian data protection authority in the context of the hearing of the parties).

The lead supervisory authority informed the Austrian data protection authority of this fact in its decision pursuant to Art. 60(3) of the GDPR. There was no reason for a relevant and well-founded objection. A legitimate grievance on the part of the complainant cannot be identified, as the purpose of the right of access is to provide a data subject with information about the personal data processed about him or her by the controller. The complainant received this (negative) information in the course of the proceedings (cf. in the national context § 24 para. 6 of the Austrian Data Protection Act, according to which a controller may subsequently remedy the alleged infringement by complying with the requests of the data subject). The fact that the information provided by the respondent was defective was not alleged by the complainant at any time.

As a result, the complainant was left without a complaint.

If a complaint is rejected or dismissed, the supervisory authority to which the complaint was lodged shall adopt the decision and notify it to the complainant and inform the controller, in accordance with Article 60(8) of the GDPR. This is the case here. For this reason, the decision in question is issued by the Austrian data protection authority.

Therefore, the decision had to be in accordance with the ruling.

GZ:D130.474
2021-0.281.893

Clerk: [REDACTED]

Data protection complaint (Access)
[REDACTED]

D E C I S I O N

R U L I N G

The data protection authority decides on the data protection complaint of [REDACTED] (complainant), dated 6 July 2020, against [REDACTED] (opponent) based in Düsseldorf, Germany, for violation of the right to access as follows:

- The handling of the complaint is rejected.

Legal basis: Art. 4 subpara 23 lit. b, Art. 51 para 1, Art. 57 para. 1 lit. f and para 4, Art. 60 and Art. 77 para 1 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter: GDPR), ABI. Nr. L 119 vom 4.5.2016 p. 1; §§ 18 para 1 and 24 para 1 and para 5 of the Data Protection Act (DSG), Federal Law Gazette I No. 165/1999 idgF.

R E A S O N S

A. Claims of the parties and proceeding

1. By initiating the proceedings of 6 July 2020, the complainant claimed an infringement of the right to access and basically argued that the respondent had only partially complied with his request of 15 May 2020.

As an attachment, the complainant submitted correspondence with the opponent.

This included the request for access dated 15 May 2020. In this request, the complainant requested payment data in connection with his master card, e-mail correspondence, contact form requests in connection with the reservation code [REDACTED], web log data in particular concerning his reservation, service center log data and audio recordings of telephone contact with the service hotline as well as other data relating to his booking. Furthermore, the complainant stated in this letter that he was willing to refrain entirely from the complete request and that he would withdraw his request as soon as the

respondent came to the conclusion that it would be more economic to comply with his and his family's claim for reimbursement of more than EUR 280 immediately. If the opponent fails to comply with his request within the time limit, he would lodge a complaint with the competent supervisory authority on 15 June 2020.

Furthermore, to the complaint was attached the respondent's reply, respectively the information requested, of 9 June 2020.

2. Since there is a cross-border situation, the Data Protection Authority placed the case in the "Internal Market Information (IMI) system", which is used in the context of the coherence procedure to process the cross-border procedure in accordance with the provisions of the GDPR. The respondent's headquarters are in Düsseldorf, Germany.

Accordingly, it had to be assumed that according to Art. 56 para. 1 GDPR, the responsible German supervisory authority, specifically the Land Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia, was the lead supervisory authority for this procedure. This circumstance was communicated to the complainant.

3. The Land Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia (LDI NRW) considered itself responsible for the handling of the complaint. The latter subsequently submitted a draft decision pursuant to Art. 60 para. 3 GDPR.

It is clear from this draft decision that an investigation has not been initiated. The opponent had fully complied with the obligation to provide information. According to the information provided, only calls from Germany are recorded and log data are processed without personal reference and there are no indications to call these statements into question.

Art. 15 GDPR regulates the right of access to personal data processed by a controller. This right is not forfeited by the fact that information is sought for a purpose other than data protection law, in particular if the parties are involved in a dispute.

However, it was questionable whether the request for information had been abusive. However, the existence of an abuse of rights can only be assumed if it is apparent from special circumstances that the request for access is aimed solely at the damage to the person responsible. One indication of this could be the complainant's intention to cause harm, which the complainant openly expresses in his request. In this respect, the complainant made a very extensive claim for information, which alone was not an indication of abuse of rights. However, in his letter of 15 May 2020, the complainant clearly pointed out that it could be more economic for the company to immediately comply with the complainant's and his family's claims for reimbursement of EUR 280. In the event of an immediate reimbursement, he would be willing to refrain from requesting the information. This approach could well

be interpreted as blackmail. The complainant thus made it clear that he would refrain from his request if his claim was met, which, in the view of the LDI NRW, constituted an abuse of law.

In view of the fact that the complainant's request for information had already been fully complied with and that the letter of 15 May 2020 also indicated an abusive intention, the complaint was not taken up in the present case.

B. Subject of appeal

The subject-matter of the complaint is whether the opponent violated the complainant's right to access pursuant to Art. 15 GDPR.

However, it must be checked in advance whether the requirements of Art. 57 para. 4 GDPR are met.

C. Findings of facts

The data protection authority shall base its decision on the facts set out in point A.

D. From a legal point of view, it follows:

The subject-matter data processing is a cross-border data processing according to Art. 4 subpara 23 lit. b GDPR, since the complainant is domiciled in Austria, the controller (opponent) is established in Düsseldorf, Germany. The leading supervisory authority is therefore the LDI NRW pursuant to Art. 56 para. 1 GDPR.

The Lead Supervisory Authority came to the conclusion that an investigation was not to be conducted, respectively that the handling of the complaint was to be rejected. This, particularly since, on the one hand, full information was given and, on the other hand, the request for access from the complainant dated 15 May 2020 indicated that the right of information was abusively exercised.

The responsible supervisory authority informed this circumstance in accordance with Art. 60 para. 3 GDPR in its decision to the Austrian Data Protection Authority. Relevant and reasoned objection were not raised.

In accordance with Art. 57 para. 4 GDPR, the supervisory authority may in cases where requests are manifestly unfounded or excessive, in particular because of their repetitive character, charge a reasonable fee based on administrative costs, or refuse to act on the request. The purpose of the right to information is that a data subject receives information about their personal data processed by a controller. On 9 June 2020, the controller had already provided full access to the complainant and the complainant had indeed stated in his request of 15 May 2020 that he would refrain from his request if he received a refund of the amount requested. The complaint therefore proves to be manifestly unfounded, why according to Art. 57 para. 4 GDPR the treatment had to be rejected.

If a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall in accordance with Art. 60 para. 8 GDPR adopt the decision and notify it to the complainant and shall inform the controller thereof. As this is the case in the present case, the decision in question is issued by the Austrian Data Protection Authority.

It was to be decided according to the ruling.

L E G A L N O T I C E

A complaint to the Federal Administrative Court may be lodged against this decision in writing within **four weeks** of notification. The complaint must **be lodged with the Data Protection Authority** and must include

- the name of the contested decision (GZ, subject)
- the name of the authority concerned;
- the grounds on which the allegation of illegality is based,
- the demand as well as
- the information necessary to assess whether the appeal has been lodged in time.

The Data Protection Authority has the option to amend its decision by means of a **preliminary complaint decision** or to **submit the complaint with the files of the proceeding to the Federal Administrative Court**.

The appeal against this decision is **subject to a fee**. The fixed fee for a corresponding submission including attachments is **EUR 30**. The fee must be paid on the account of the Austrian Tax Office, stating the purpose of use.

The fee must in principle be transferred electronically with the function “Finanzamtszahlung”. As recipient, the Austrian Tax Office – Department of Special Responsibilities should be indicated or selected (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). Furthermore, the tax number/tax account number 10 999/9102, the type of fee “EEE-Beschwerdegebühr”, the date of the decision as the period and the amount must be indicated.

If the e-banking system of your credit institution does not have the function “Finanzamtszahlung”, the eps procedure can be used in FinanzOnline. From an electronic transfer can only be refrained if no e-banking system has been used (even if the taxable person has an internet connection). Then the payment must be made by means of a payment order, taking care of the correct attribution. Further information can be obtained from the Tax Office and in the manual *“Elektronische Zahlung und Meldung zur Zahlung von Selbstbemessungsabgaben”*.

The payment **of the fee shall be demonstrated** when the complaint is lodged with **the data protection authority** by means of a payment document to be followed by the submission of a payment order or an expression of the issue of a payment order. If the fee is not paid or not paid in full, a **notification will be sent to the competent Tax Office.**

A timely and admissible appeal to the Federal Administrative Court has **suspensive effect**. The suspensive effect may have been excluded in the statement of the decision or may be excluded by an own decision.

3. Mai 2021

For the head of the Data Protection Authority:

[REDACTED]

GZ:D155.011

DSB-D155.011/0003-DSB/2019

Sachbearbeiterin)Mag. [REDACTED]

«Anrede»

«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»

«Name»

zH «zH»

«Straße» «ON»

«Postleitzahl» «Ort»

«Land»

Formal examination procedure

[REDACTED] (IMI-Nr.: A56ID 67978)

Subject: Closing of proceedings

1. The Austrian Data Protection Authority received the submission of [REDACTED] dated on 2 August 2018, which was submitted by the Land Commissioner for Data Protection and Freedom of Information in Baden-Württemberg on 29 May 2019.
2. In accordance with Art. 56 (1) in conjunction with Art. 60 GDPR, the Austrian data protection authority is the leading supervisory authority in this cross-border procedure.
3. In the submission it was stated that the [REDACTED] demanded on their website with a banner the consent to the use of cookies and the option for a “pure subscription”, which allows the use of the website without advertising and without cookies. It was assumed that the website could also be operated without cookies and they were not mandatory for this. However, the user was not given the opportunity to allow advertisements for the financing of the website without using cookies, which indicates a violation Art. 7 (4) GDPR. The submission also asked for an examination of this matter.
4. The Austrian Data Protection Authority assumed that this submission was a request for an ex-officio- proceeding.
5. On 2 August 2019, the Austrian Data Protection Authority requested the opinion from [REDACTED] within 3 weeks.

6. No comments were made within this period.

7. In its decision of 30 November 2018, the Austrian Data Protection Authority DSB-D122.931/0003-DSB/2018¹ already agreed on the voluntary consent to the use of the cookie in question by [REDACTED]
[REDACTED]

8. The Lander Commissioner for Data Protection and Freedom of Information Baden-Wurtemberg agreed to close the procedure via IMI on the 25. March 2021.

9. Therefore, the Austrian Data Protection Authority thinks there is no need initiate another ex-officio-proceeding about this matter and closes the procedure.

17.05.2021

Für die Leiterin der Datenschutzbehörde:

[REDACTED]

¹See

https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_2018_1130_DSB_D122_931_0003_DSB_2018_00.pdf.

GZ:D155.018
2020-0.339.292

SachbearbeiterinMag. [REDACTED]

«Anrede»
«Titel»«Vorname»«Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße»«ON»
«Postleitzahl»«Ort»
«Land»

Data protection complaint (Art. 6 GDPR, Art. 13 GDPR, Art 14 GDPR)

[REDACTED] (IMI Nr.: A56ID 99607); Case Nr. 112370

by e-mail «emailadresse»

FINAL DECISION

The data protection authority decides on the anonymous data protection complaint, received by the Slovenian supervisory authority on 1 February 2020, against [REDACTED] (opponent) for 1) an infringement of the right to information and 2) an infringement of the right to legality of processing as follows:

— The complaint is dismissed as unfounded.

Legal basis: Art. 6, Art. 12, Art. 13, Art. 14, Art. 51, Art. 56, Art. 57 para 1 lit. f, Art. 60 and Art. 77 GDPR regulation (EU) 2016/679, published in the Journal of the European Union Nr. L 119 from 4th of May 2016, p. 1.

REASONING

A. Arguments of the parties and course of proceedings:

1. The austrian data protection authority was notified by the Slovenian supervisory authority according to Art. 56 iVm At.60 GDPR of 28 February 2020 on the basis of an anonymous complaint dated 1. February 2020, that the opponent in his Slovenian branch had monitored the internet use of employees with regard to the visited websites and the amount of data usage as well as their professional e-mails.

The specific statistics on Internet use, including the website domains, were available to employees for their own use. Furthermore, the employees were not informed of such processing in accordance with Articles 13 and 14 GDPR.

2. As this is a cross-border case, the Slovenian supervisory authority placed the case in the “Internal Market Information (IMI) System”, which is used in the cooperation procedure to manage **cross-border cases** under the provisions of the GDPR. It turned out that the main establishment of the controller, [REDACTED], commercial register number [REDACTED], is at address [REDACTED], Austria, so that the Austrian data protection authority is the lead supervisory authority in this case pursuant to Article 56(1) GDPR. Due to the fact that the opponent [REDACTED] has further establishments in Member States of the European Union, in particular in Croatia, Hungary and Slovakia, the supervisory authorities of these countries had to be included as concerned supervisory authorities pursuant to Art. 4.22 DSGVO.

3. At the request of the Austrian data protection authority dated 28 February 2020, the opponent stated in its submission from 20 May 2020 that the opponent had obtained its IT infrastructure services from [REDACTED] (processor) and that this processor had automated personal log files on the proxy server for IT security reasons. Access to the Internet communication of the employees is only permitted for the course of investigations in case of malfunctions or for the detection of security incidents and requires an appropriate authorisation of selected department heads or managing directors. It was correct that the processor recorded the total volume of Internet traffic caused by the opponent's employees, i.e. the amount of data used for the purpose of billing between the opponent and the processor. It is also true that the Internet traffic caused by individual employees on the intranet was represented by a “traffic light system” to the respective employee, but it did not show the websites visited by the user or other content data. This system had been introduced by above-average Internet traffic due to significant problems in the past. Due to the Covid 19 pandemic, the entire traffic light system had now been removed from the opponent's intranet. All employees were informed about the traffic light system by the Group Data Protection Officer. With regard to the “statista” link, the opponent did not at any time commission the alleged monitoring or logging of the employees' websites accessed. The factual logging of the websites accessed was created by the processor for internal reasons and was limited to their employees. For this purpose, the necessary company works agreement had been obtained. Apparently, a misadjustment had led to an employee having accessed his own statistics. However, it was not possible to receive the statistics of another employee. The opponent had prompted the immediate deactivation of the “statista” link for its employees and the deletion of all recorded data. The concrete legal basis for the logging of the data generated by the respondent and the traffic light system is Art. 6 (1) (f) GDPR, according to which the opponent's legitimate interests outweigh, because of the billing of the internet connection between the opponent and the processor, which was dependent on the opponent's Internet usage. The traffic light system was used for easy self-regulation of the opponents employees. A data protection assessment had not been carried out because it had fallen

under the electronic communication tools under DSFA-A20 (WP29, guidelines on data protection impact assessment (DSFA) etc.). The opponent did not see the need for an assessment of data protection due to the lack of intervention-intensive design, the strict access rules and, because this did not involve systematic monitoring. With regard to the alleged monitoring of the e-mail communication by the opponent's staff, the opponent informed that such a communication had not taken place. The only access to user-related e-mail mailboxes was through a common support system in case of technical errors via a ticket system. The processor had confirmed that there were no requests for "opening" (inspection) in e-mail accounts by the opponent.

4. The respondent's comments were forwarded to the Slovenian supervisory authority on 17 July 2020.

B. Subject of complaint

In the present case, the question arises as to whether the opponent's employees of the Slovenian branch have been infringed in their rights to information and whether the principles relating to processing of personal data and the lawfulness were infringed in accordance with Art. 6, Art. 12, Art. 13 and Art. 14 GDPR by monitoring the Internet use and the e-mail traffic of the opponent's employees.

C. Findings of the case:

1. Within its group and in its Slovenian branch [REDACTED], banking subsidiary, [REDACTED], [REDACTED], the opponent has installed a "traffic light system" which was made available by its processor, [REDACTED], from which the opponent receives its essential IT infrastructure services, at least until 24 October 2019. This processor records the total volume of Internet traffic caused by the opponent's employees, i.e. by the opponent's IT systems, for the purpose of billing, since the opponent's billing results in gigabytes of internet volume per month and quarter. In addition, there have been considerable problems in the past due to above-average Internet usage by individual employees. Therefore, the traffic light system was introduced, which only indicates the generated Internet traffic of the individual employee and serves them for self-control.

2. The respondent's employees were informed about the traffic light system, which displays their generated Internet traffic by means of data protection information via intranet and in the context of mandatory data protection training, as well as the data protection information for opponent's employees: (Excerpt, formatting not returned 1:1):

Datenschutzinformation für Mitarbeiter 2/2

- Inwieweit gibt es eine automatisierte Entscheidungsfindung – findet Profiling statt?
- Information über Ihr Widerspruchsrecht
- Persönlicher E-Mail-Account, Passwort, Berechtigungen, Mitarbeiter-Zutrittskarte (Verweis auf das HB IKT Security)
- Selbstkontrolle der Internetnutzung (Ampel im Intranet)
- Datengeheimnis Geheimhaltungsverpflichtung
- Verschwiegenheitsverpflichtung: Betriebsgeheimnisse, Geschäftsgeheimnisse, Geistiges Eigentum, Urheberrechtliche Informationen Datengeheimnis

Die Datenschutzinformation für Mitarbeiter ist im Intranet unter [REDACTED]
[REDACTED] jederzeit abrufbar!

3

Erhebung von Daten aus anderen Quellen (Art. 14 DSGVO)

Überdies erlangen wir Daten aus unseren technischen Systemen der IT-Infrastruktur. Wir verarbeiten in diesem Zusammenhang folgenden Kategorien von Daten: technische Logdaten und Protokolldaten, nämlich Datum, Uhrzeit, E-Mail-Adresse von Sender und Empfänger oder Username, Nachrichtengröße von E-Mails und im Logfile der Internetnutzung (Proxy-Log) werden IP-Adresse, von der aus die Internetnutzung erfolgt, IP-Adresse des aufgerufenen Servers, abgefragte Seiten, Datenvolumen, Datum und Uhrzeit und Benutzername des abfragenden Benutzers protokolliert. Die Verarbeitung dieser Daten erfolgt auf Basis berechtigter Interessen im Rahmen einer Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO), wobei unser berechtigtes Interesse sowie die verfolgten Zwecke in der Abrechnung der IT-Dienstleistungen mit unseren IT-Dienstleistern, insb. der [REDACTED] der Aufrechterhaltung der IT-Sicherheit sowie der Verhinderung und Aufklärung von Straftaten oder schwerwiegenden Pflichtverletzungen liegen.

3. The Slovenian supervisory authority received complaints that the internet use and e-mail traffic of the opponent's employees had been monitored by the opponent, which prompted the Slovenian supervisory authority to initiate proceedings and they carried out an on-the-spot inspection procedure at the opponent's Slovenian branch on 24 October 2019.

4. As part of the on-the-spot inspection procedure, it was found that the employees on the intranet under the title "Internet use" ("traffic light system") had an indicator of their own Internet use (*emphasis by the data protection authority, formatting not returned 1:1*):

[REDACTED]

INFORMATIONSPORTAL für [REDACTED]

Donnerstag, 24. Oktober 2019 |

STÖRUNG: Systemprobleme Kondor
ZBE, Fr. [REDACTED] 79436:
Systemprobleme Kondor
An der Störungsbehebung wird bereits gearbeitet.
Beginn der Störung: 24.10.2019, 10:08 Uhr

Verpflichtende PIN-Eingabe im SB-Bereich (Betrifft: Vertrieb)
ZBE, Hr. [REDACTED] 79437:
Seit 24.10.2019 ist es bei allen SB-Geräten (außer Münzeinzählern) notwendig, dass der Karteninhaber sich mit der PIN identifiziert. Einzige Ausnahme: bei Einzahlungen - hier ist die PIN-Eingabe nicht notwendig.
Grund für die Änderung: Wahrung von Datenschutz und Bankgeheimnis; Schutz vor Missbrauch der Kundendaten

Checkliste Sicherheiten
ZKM, Fr. [REDACTED] 79129:
Die Checkliste Sicherheiten wurde im Punkt „Grundbürgerliche Sicherheiten“ ergänzt:
Bei der Einstiegabe der Sicherheit ist nur das Feld „Datum GB-Prüfung“ zu füllen (die Felder „Prüfintervall“ und „Letzte Prüfung am“ sind auf Grund der autom. Compasseinschränkungen nicht zu befüllen).
Bei hypothekarischen Sicherheiten ob ETW ist zwingend auch das TOP im SICH aufzugeben. Bei noch nicht parifizierten Wohnenheiten, z.B. Bauträgerprojekten, können sich so die LBW-Schätzung und die entsprechende Sicherheit finden, wenn zwar die B-LNr fehlt, aber das TOP in beiden Systemen aufgegeben ist.

Mittwoch, 23. Oktober 2019 |

Segmentierung FK & GK (KSM-Kampagne)

5. Statistics on the specific amount of data used by the respective employee and the average monthly use of the data at the level of the banking group are available under <http://statistica/proxystats>. There is also a link “Request Top Sites Report” (*formatting not returned 1:1, highlights by the data protection authority*):

[REDACTED]



Statistica

Ihre Internet-Nutzung

Internet-Datenvolumen Ihres Benutzers im aktuellen Monat

Benutzername Datenvolumen in MB Richtwert in MB (Median) vom Vormonat
y195jer 1138 438

Detailreports ihres Benutzers anfordern

- [Top Sites Report anfordern](#)
- [Private Top Sites Report anfordern](#)

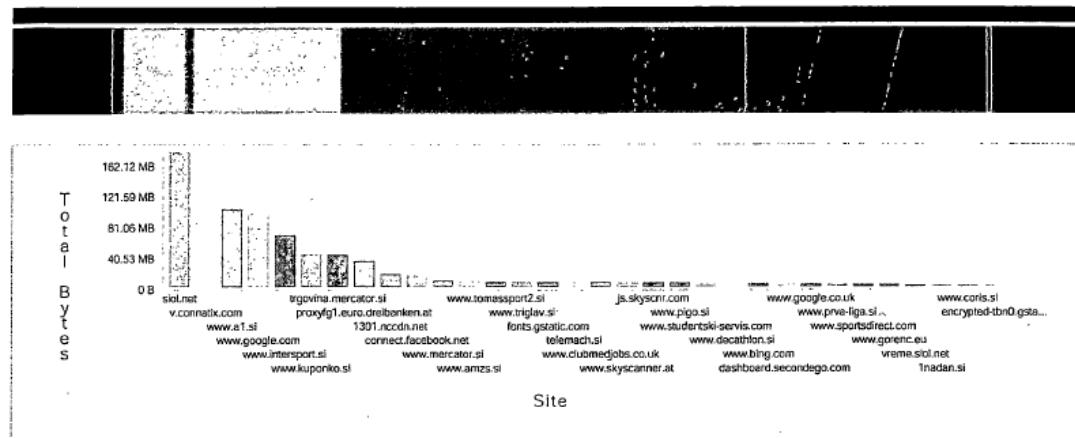
[zurück zu Internet-Nutzungsstatistiken](#)

Daten zuletzt aktualisiert am 24.10.2019 um 10:01:25 Uhr.
angemeldet als [REDACTED]
Statistica Version 1.0 - © 2011 3BEG, Ing. [REDACTED]

6. By clicking on the link (“Statista” link), an employee of the opponent was able to receive an e-mail with a PDF report on the websites he visited by himself. It was not possible to access reports from other

employees. The report only shows the main domain of the websites visited and not the specific websites. This link was not designed for the opponent's employees and was not commissioned by the opponent, but had been created by the processor for internal security reasons. In order to ensure traceability in the event of a security incident, which connections are made from which systems to the Internet, user name, IP address, searched pages, data volume, date and time have been stored in a "proxy log". The opponent was not aware of the "Statista" link. How the link reached an employee of the opponent can no longer be determined.

Top Sites Report - yl95jer: Calculated by Total Bytes



Report Filter: Date is Current and Previous 0 months (2019-10-01 - 2019-10-24) where Verdict is "allowed" and User Is "yl95jer"

Site	Requests	Page Views	Total Bytes
siol.net	624	0	176.61 MB
v.connetix.com	4	0	131.01 MB
www.a1.si	4,016	27	103.67 MB
www.google.com	764	12	97.81 MB
www.intersport.si	3,224	154	70.02 MB
www.kuponko.si	1,223	25	45.67 MB
trgovina.mercator.si	9,840	58	45.50 MB
proxyfg1.euro.dreibanken.at	173	0	37.19 MB
1301.nccdn.net	608	0	20.57 MB
connect.facebook.net	366	0	18.78 MB
www.mercator.si	826	23	12.36 MB
www.amzs.si	293	9	11.26 MB
www.tomassport2.si	560	107	10.44 MB
www.triglav.si	501	3	10.05 MB
fonts.gstatic.com	454	0	9.83 MB
telemach.si	145	8	9.74 MB
www.clubmedjobs.co.uk	165	8	9.66 MB
www.skyscanner.at	898	25	9.13 MB
js.skyscnr.com	458	0	8.92 MB
www.pigo.si	2,259	87	8.89 MB
www.studentski-servis.com	70	0	8.25 MB
www.decathlon.si	265	23	8.10 MB
www.bing.com	51	0	7.79 MB
dashboard.secondego.com	351	81	7.53 MB
www.google.co.uk	22	0	7.37 MB
www.prva-liga.si	1,044	13	6.93 MB
www.sportsdirect.com	50	0	6.92 MB
www.gorenc.eu	500	13	6.84 MB
vreme.siol.net	2,322	0	6.50 MB
1nadan.si	372	2	6.33 MB

Top Sites Report - yl95jer, Page: 1
Generated by queryuser via Symantec Reporter on 24/Oct/2019

7. As of May 19, 2020, the "Statista" link was deactivated and the resulting evaluations were deleted.

8. As of 8 May 2020, the “traffic light system,” on the opponent’s staff’s intranet was removed (*formatting not 1:1; highlights by the opponent:*

The screenshot shows a company intranet page with several sections of text. A red arrow points to the 'CAR-Druck Kontovertrag - Verbrauchergeschäft' section, highlighting the word 'Ampel entfernt'. Other visible sections include 'Anpassung der abweichenden Daueraufträge' and 'WARTUNG - Softwareverteilung'.

Anpassung der abweichenden Daueraufträge (Zielgruppe: Filialen mit Safes)
ZVV, Fr
Die Daueraufträge und Lastschriften bei SAFE- Standardgebühren lt. Preisaushang wurden bereits im April 2020 automatisch angepasst.
Für die handische Anpassung der abweichenden Safemieten steht Ihnen die Excel-Daten auf [BKS Global/Teamwork/Statistikdaten/Sale ab sofort zur Verfügung](#).
Die Details zur handischen Anpassung der abweichenden Mieten finden Sie in der [Beilage](#).

WARTUNG - Softwareverteilung (Zielgruppe: Notebook-User)
ZBE, Hr. MSc. BA (Econ.)
In den Nächten vom 10.-13.05.2020 ist eine flächendeckende SW-Installation per Wake on Lan in den 3 Banken vorgesehen. Bitte sorgen Sie dafür, dass Ihr N
Für jene Mitarbeiter welche mit Stand-PCs arbeiten erfolgt die SW-Verteilung ohne Benutzerinteraktion.
INFO: Notebooks, die zu diesem Zeitpunkt nicht im Netzwerk sind (w/ HomeOffice), erhalten die Updates bei der nächsten Anmeldung.

CAR-Druck Kontovertrag - Verbrauchergeschäft
Z2U, Fr
Der Kontovertrag kann wieder gedruckt werden.
Ampel entfernt

Druck Kontovertrag - Verbrauchergeschäft
Z2U, Fr
Der Kontovertrag kann aufgrund eines technischen Problems nicht gedruckt werden. An der Lösung wird gearbeitet. Wir informieren Sie, sobald der Druck wieder

LOSUNG- AFM Forms offline
ZBE,
AEM Forms offline.
Beginn der Störung: 08.05.2020 08:30
Ende der Störung: 08.05.2020 09:31

Überblick über die aktuellen WP-Vertriebsschwerpunkte
ZVV,
0,60%
0,375%

9. The only access to user-related e-mail mailboxes by others is within the framework of a usual support system, where employees can report technical errors via a ticket system. The access to the e-mail mailboxes of the opponent’s employees is only possible via the processor, which needs this access option in order to eliminate any IT malfunctions. For 2019, the processor has not received requests for “opening” (inspection) in e-mail accounts by the opponent, neither from the main establishment nor from the opponent’s branches abroad.

Appraisal of evidence: The evidence of the uncontested facts were taken from the submissions of the Slovenian supervisory authority and the respondent. The findings on points 6, 7 and 8 are based on the credible written statements of the processor.

D. Legal conclusions:

A. General information:

1.On accountability iSd.Art. 4 subpara 7 GDPR

This is a cross-border procedure, which must be handled in accordance with the provisions of the GDPR. The opponent's main office is [REDACTED], company book number [REDACTED], address [REDACTED] Austria so that the Austrian data protection authority is the leading supervisory authority in accordance with Article 56(1) of the GDPR. The Austrian opponent is the head office of the group, which makes the main management decisions for the purposes and means of processing the personal data of its employees in the branches in Austria, Slovenia, Slovakia, Hungary and Croatia. The opponent is, therefore, the responsible party according to Article 4 (7) GDPR.

2.On the existence of personal data:

Personal data according to Art. 4 (1) GDPR is all information relating to an identified or identifiable natural person. Identifiable shall be considered to be a natural person who is directly or indirectly expressing the physical or social identity of that natural person, in particular by assigning it to an identifier such as a name [...] or to one or more specific characteristics, which are an expression of the physical [...] or social identity of that natural person.

In the case of e-mails as well as the present „traffic light system” and the data of the “statista” link, through which the internet use of the respective employees is processed, it is undisputed personal data according to Art. 4 (1) GDPR, since the individual employees, or their Internet usage, are identifiable.

B. On the alleged breach of the duty of information pursuant to Art. 13 and Art. 14 GDPR:

In the present case it was claimed that the employees were not informed about the processing of their Internet usage data.

Art. 13 and 14 GDPR are to be understood as the basis for the data subject's rights in accordance with Chapter III (rights of the data subject) GDPR, since the data subject first learns that data is processed by a particular controller about him/her. Also the Recital 60 GDPR refers to the principle of fair and transparent processing, which enables the data subject to be informed of the existence and purposes of the processing process. The importance of informing the parties concerned is also emphasised by the ECJ in its case law (cf. on the legal situation under Directive 95/46/EC the judgment of 1 October 2015, C-201/14).

The date to inform the data subject is according to Art 13 (1) GDPR the time when the personal data is obtained. The date of the collection may also be when the person concerned knowingly gives data to

the person responsible (*Knyrim in Ehmann/Selmayr (ed.)*, General Data Protection Regulation, Art. 13, Rz. 11).

While Art. 13 GDPR regulates the case that the data is collected directly from the data subject, Art. 14 GDPR regulates cases in which the data is not collected from the data subject (*Knyrim in Ehmann/Selmayr (ed.)*, General Data Protection Regulation, Art. 14, Rz 2).

The opponent was able to provide credibly and substantiate evidence that the employees have become aware of the “traffic light system” or the collection of their internet usage via intranet, as well as by the group data protection officer, in the context of an obligatory data protection training, as well as the general data protection information for employees of the processing of their data in a transparent and understandable manner pursuant to Art. 12 (1) GDPR. Thus, there is no violation of the right to information relating to the processing of employee data about their Internet use in accordance with Articles 13 and 14. GDPR.

C. On the legality of processing:

1. On the alleged monitoring of the Internet usage:

In accordance with Art. 6 (1) (f) GDPR, processing is lawful if the processing is necessary to safeguard the legitimate interests of the controller or a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data prevail.

As a result, a balance of interests must be carried out in accordance with Art. 6 (1) (f) GDPR. If the processing of the data in question was necessary to safeguard the legitimate interests of the controller or a third party, this may be justified unless the interests of the complainant outweigh. Consideration must be given to the content and significance of the data concerned as well as to the purpose of processing (*Buchner/Petri in Kühling/Buchner*, General Data Protection Regulation, Rz 149). Additionally the expectations of the data subject must be considered according to Rec. 47 of the GDPR, in particular whether the data subject reasonably had to expect further processing at the time of the collection of the data.

As stated, the basis for the billing between the opponent and its processor is the volume of Internet data consumed in the group. Therefore, there have been problems in the past due to above-average data use by individual employees.

The opponent's legitimate interest in installing a system that warns employees at high data consumption through a traffic light system is to achieve the fairest possible balance of data consumption between employees and to introduce a cost-limiting measure by simple self-regulation. Especially since the opponent has provided Internet access for service purposes and the processor has credibly submitted that the evaluations of the website visits (“statista” link) of the individual employees were not

commissioned by the opponent, who had not even been aware of it. The statista link was only used for internal IT security purposes by the processor.

On the other hand, the employee's legitimate interests lie in the protection of their personal data in accordance with Art. 8 EU-CFR, whereby the employees could expect the processing in question for security purposes and cost limitations.

In the present case, the Austrian data protection authority considers the interests of the employees to be safeguarded and considers that the secrecy interest of the employees in their use of the Internet for work-related reasons should not be given more importance than the opponent's interest in limiting costs and fair balance between employees and the need of the processor to store the requested pages of the employees ("proxy log") for the purpose of IT security.

2. On the alleged monitoring of e-mail correspondence:

As stated, there are no concrete indications that in 2019 the opponent made use of its access to the e-mails of its employees via the processor who supervised the entire IT infrastructure. Thus, the data protection authority could not find evidence of the monitoring of the e-mail correspondence through the opponent.

Pursuant to Art. 60.8 GDPR, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof. As stated, the complaint was anonymous, therefore the Slovenian supervisory authority is not obliged to notify the unknown complainant.

30. Juni 2021

Für die Leiterin der Datenschutzbehörde:

[REDACTED]



Republik Österreich

Datenschutz
behörde

Barichgasse 40-42

A-1030 Wien

Tel.: +43-1-52152 302564

E-Mail: dsb@dsb.gv.at

GZ: D130.288
2021-0.370.925

clerk: Mag. [REDACTED]

Data protection complaint (Right to erasure)
[REDACTED]

Betreff: notice; closing of the proceedings

By letter dated 22.05.2021, the complainant announced that she withdraws her complaint.

The proceedings were therefore to be ended informally (without a decision) and the data protection authority hereby brings this to your attention.

14. Juli 2021

For the head of the Data Protection Authority:
[REDACTED]

GZ:D155.022
2021-0.540.987

SachbearbeiterinMag. [REDACTED]

Notification of personal data breaches to the supervisory authority
(Art. 33 GDPR, "Data-Breach-Procedure")

[REDACTED] (IMI Nr.: A56ID 123192)

Draft Decision

By notification of 18 March 2020 as well as the follow-up reports of 26 March 2020 and 23 April 2020, [REDACTED] (controller) informed the Austrian Data Protection Authority on a breach of the protection of personal data.

In summary, on March 16, 2020, the controller noted a cyber attack as there was an increased activity (number) of user access requests that caused user authentication errors. The attackers had obviously obtained the names and passwords of the concerned accounts before the authentication attempt and were able to access 624 user accounts, 97 of which were from the European Union.

The concerned individuals are residing in the following EU countries: Croatia, Germany, Austria, Belgium, Denmark, Italy, Sweden, Romania, Poland, Hungary, Spain, France, the Netherlands and Portugal.

A total of 624 Users, 97 of them based in the E.U., were affected by the incident.

The data of the categories

- Usernames (email address) and passwords (known to the attacker before the attack)
- User device type (Android device, iOS device)
- Application program (iTranslate iOS, iTranslate android)
- User_ID
- Newsletter subscribed (Yes, No)
- Installation_ID

have been affected.

The person responsible has taken the following measures to remedy the injury or mitigate possible adverse effects:

- After discovering the unusual activities, access has been blocked and passwords have been reset.
- An e-mail has been send to the affected customers to inform them about the incident and the measures taken. It was recommended to them to change their passwords.

The responsible parties have taken the following measures to prevent such incidents in the future:

- A new patch has been installed to block suspicious IP addresses after a failed authentication attempt.

The controller has taken appropriate steps to minimise the risk and to eliminate, as far as possible, the adverse consequences of the security breach. Further measures of the data protection authority according to Art. 58 para. 2 lit. e GDPR or § 22 para. 4 DSG are not required.

The procedure will therefore be closed and the controller will be notified thereof.

4. August 2021

Für die Leiterin der Datenschutzbehörde:

[REDACTED]

GZ: D155.050
2021-0.657.376

Sachbearbeiter Mag. [REDACTED]

«Anrede»
«Titel» «Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

Data protection complaint (Art. 17 GDPR, Right to erasure)

[REDACTED] (AD56ID 180521)

by RSb/letter/email «emailadresse»

Subject: Final Decision

The complainant [REDACTED] lodged a complaint (at the Austrian Data Protection Authority on 26 March 2021) against [REDACTED] (the respondent) against the Data Protection Authority, claiming an infringement of the right to erasure (Art. 17 GDPR) by not responding to its request of September 2020.

By letter of 6 July 2021, the respondent responded to the complainant's request for deletion in the ongoing proceedings before the Data Protection Authority (which subsequently eliminated the alleged infringement of the non-delivery deletion). Thus, an amicable agreement could be reached between the appellant and the respondent.

The complainant did not dispute the access of this letter in the party hearing granted to it and, despite the request to that effect, did not make any further submissions. A corresponding forwarding report is attached to the act and there is no error message of an email server.

Accordingly, the appeal proceedings had to be closed informally (without any decision).

Genehmigungsdatum

Für die Leiterin der Datenschutzbehörde:

Genehmiger(in)



Republik Österreich

Datenschutz
behörde

Barichgasse 40-42

A-1030 Wien

Tel.: +43-1-52152 302583

E-Mail: dsb@dsb.gv.at

GZ: D130.352
2022-0.052.510

Sachbearbeiter: [REDACTED]

[REDACTED]
Data protection complaint (Right of Access)

per RSb/Brief/E-Mail «emailadresse»

D E C I S I O N

The data protection authority decides on the data protection complaint of [REDACTED] (complainant) of 2 December 2019 against [REDACTED] (respondent) for violation of the right of access as follows:

- The complaint is dismissed.

Legal basis: Art. 15, Art. 51 para. 1, Art. 57 para. 1 lit. f, Art. 60 para. 8, Art. 77 para. 1 and Art. 85 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter: GDPR); § 18 para. 1 and 24 para. 1 and para. 5 of the Data Protection Act (DSG)

J U S T I F I C A T I O N

A. Arguments of the parties and course of proceedings

1. By complaint of 2 December 2019, as amended by submissions of 28 January 2020 and 2 March 2020, the complainant alleged a violation of the right of access because the respondent had not responded to her request for information.
2. As the case involved a cross-border issue, the DPA placed the case in the Internal Market Information (IMI) system, which is used under the consistency mechanism to handle the cross-border procedure under the provisions of the GDPR.
3. The head office of the respondent is in the Netherlands, which is why the Dutch supervisory authority (Autoriteit Persoonsgegevens) was the lead supervisory authority in these proceedings pursuant to Article 56(1) GDPR.

The Dutch supervisory authority considered itself competent to deal with the substance and forwarded the complaint to the respondent.

4. The lead supervisory authority subsequently submitted a draft decision to the data protection authority pursuant to Article 69 (3) of the GDPR by letter of 18 November 2020. This shows that on 31 October 2019, the respondent requested the complainant's representative to provide proof that he had been mandated as an authorised representative on behalf of the complainant. No reply had been received.

The respondent further stated that it had received confirmation on 30 October 2020 that the requested proof would be sent by the complainant.

According to Article 12 of the GDPR, it is permissible for a controller to request additional information if the controller doubts the identity of the data subject.

The Dutch supervisory authority could not find a violation of the GDPR.

B. Subject matter of the complaint

The subject matter of the complaint is whether the respondent infringed the complainant's right of access under Article 15 GDPR.

C. Findings of fact

The data protection authority bases its decision on the facts of the case as set out in point A. and documented in the file.

D. From a legal point of view, the following follows:

The data processing subject of the complaint is a cross-border data processing within the meaning of Article 4(23)(b) of the GDPR, as the complainant is domiciled in Austria, but the controller (respondent) is established in the Netherlands. The lead supervisory authority was therefore the Dutch supervisory authority pursuant to Art. 56(1) GDPR.

In the course of the proceedings, the lead supervisory authority came to the conclusion that no violation of the GDPR had occurred.

The lead supervisory authority informed the Austrian data protection authority of this fact in its decision pursuant to Article 60 (3) of the GDPR. There were no grounds for an authoritative and substantiated appeal.

If a complaint is rejected or dismissed, the supervisory authority to which the complaint was submitted shall adopt the decision and notify the complainant and inform the controller, in accordance with Article 60(8) of the GDPR. This is the case here. For this reason, the decision in question was issued by the Austrian data protection authority.

Therefore, the decision had to be made in accordance with the ruling.

I N F O R M A T I O N O F L E G A L R E M E D I E S

An appeal against this decision may be lodged in writing with the Federal Administrative Court within four weeks of notification. The complaint must be lodged with the data protection authority and must include

- the name of the contested decision (GZ, subject)
- the name of the authority being prosecuted,
- the grounds on which the allegation of illegality is based,
- desire and
- the information necessary to assess whether the complaint has been lodged in good time.

The data protection authority may within two months either amend its decision by means of a preliminary decision on the complaint or submit the complaint with the files of the proceedings to the Federal Administrative Court.

The appeal against this decision is subject to a fee. The fixed fee for a corresponding submission including enclosures is 30 euros. The fee is to be paid into the account of the tax office for fees, transaction taxes and gambling (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW), whereby the respective appeal procedure (business number of the notice) is to be stated as the purpose of payment on the payment order.

In the case of electronic transfer of the appeal fee with the "tax office payment", the tax office for fees, transaction taxes and gambling (IBAN as before) must be stated or selected as the recipient. In addition, the tax number/tax account number 109999102, the tax type "EEE - complaint fee", the date of the notice as the period and the amount must be stated.

The payment of the fee must be proven to the data protection authority when the complaint is lodged by means of a original payment receipt confirmed by a postal office or a credit institution, which must be attached to the submission. If the fee is not paid or not paid in full, a report is sent to the competent tax office.

A timely filed and admissible appeal to the Federal Administrative Court has suspensive effect. The suspensive effect may have been excluded in the ruling of the decision or may have been excluded by a separate decision.

January 21, 2022

For the head of the data protection authority





Republic of Austria

Data Protection
Authority

Baichgasse 40-42
A-1030 Vienna
Tel.: + 43-1-52152 302597

E-mail: dsb@dsb.gv.at

GZ: D130.1251
2023-0.585.041

Clerk: [REDACTED]

Data protection complaint (Art. 5 and 6 GDPR)

[REDACTED] and [REDACTED] (IMI No. A56ID 450784)

FINAL DECISION

VERDICT

The Austrian Data Protection Authority decides on the data protection complaint of [REDACTED] and [REDACTED] (complainants) of 2 August 2022 against [REDACTED] (respondent) for alleged breach of the general principles and the legality of the data processing pursuant to Art. 5 and Art. 6 GDPR as follows:

- The complaint is dismissed.

Legal basis: Articles 2, 4(7), 5, 6, 51(1), 56, 57(1)(f), 60 and 77(1) of Regulation (EU) 2016/679 ('General Data Protection Regulation': GDPR), OJ L 119 of 4.5.2016 p. 1; §§ 18(1) and 24 (1) and (5) of the Austrian Data Protection Law (DSG), Federal Law Gazette I No. 165/1999 as amended; § 45 (2) of the General Administrative Procedure Act 1991 (AVG), Federal Law Gazette No. 51/1991 as amended.

REASONING

A. Arguments of the parties and the proceeding of the proceedings

1. The complainants claimed in the appeal initiating the proceedings of 2 August 2022, improved with submissions of 18 August 2022, 14 September 2022 and 16 November 2022, a breach of the general principles and the lawfulness of the data processing, alleging, in summary, that the respondent had disclosed the complainants' personal data to third parties. The complainants had met the respondent through an online congress and then booked two sessions with her. Subsequently, there were disputes over the recovery of the fee because the complainants felt betrayed by the respondent. A few weeks later, the complainants were unable to view Facebook content of a third person they would follow, namely [REDACTED]. [REDACTED] had informed the complainants that she had blocked the complainants on Facebook because she was a very good friend of the respondent and could not remotely understand the complainants' actions against the respondent. Although [REDACTED] informed the complainants that she had learned about these circumstances by detours, it was clear to the complainants that the respondent had passed on personal details to third parties. There may also be a reputational damage. The complainants submitted undated text messages of [REDACTED] [REDACTED] and subsequently a power of attorney from [REDACTED] for [REDACTED] regarding the proceedings at issue.

2. By decision of 28 November 2022, CZ: D130.1251 (2022-0.820.918), the Data protection authority suspended the present proceedings until the finding of the lead supervisory authority and until the decision of the lead supervisory authority or of the European Data Protection Board in accordance with Article 56(1) GDPR in conjunction with § 24(10)(2) of the DSG.

3. The Data Protection Authority submitted in the Internal Market Information System of the European Union ("IMI") under IMI 450784 a notification of the present complaint and initiated the investigation of the lead and the concerned supervisory authority(s) in accordance with Art. 56 GDPR.

4. The State Commissioner for Data Protection and Freedom of Information Mecklenburg-Vorpommern confirmed its role as the lead supervisory authority in the present case, opened the investigation procedure and submitted a draft provisional decision to the Data Protection Authority under IMI 482366 on 1 February 2023. The draft decision proposed the rejection of the present complaint. In summary, it was stated that the data processing at issue falls under the so-called "household-exemption" in accordance with Article 2(2)(c) GDPR.

5. The Data Protection Authority responded to the State Commissioner for Data Protection and Freedom of Information Mecklenburg-Vorpommern on 17 February 2023 under IMI 482366, in the context of the informal consultation, that it could not follow the draft decision, since the facts were not sufficiently clear and, based on the given information at that time, it could not be clearly stated that the alleged disclosure of data did not take place in a professional context. The State Commissioner for Data Protection and Freedom of Information Mecklenburg-Vorpommern was therefore requested to set further investigative measures with regard to the motive for the alleged disclosure of data and to possible

data processing within the so-called “household-exemption” pursuant to Article 2(2)(c) GDPR.

6. With notification of 18 July 2023, the State Commissioner for Data Protection and Freedom of information Mecklenburg-Vorpommern submitted to the data protection authority under IMI 539360 a new draft decision including correspondence with the respondent as part of its further investigative measures. The new draft decision also proposed the rejection of the present complaint. In summary, it was stated that the further investigative measures did not provide any evidence for the disclosure of data claimed by the complainants, which would fall under the scope of the GDPR.

7. The Data Protection Authority responded to the State Commissioner for Data Protection and Freedom of information Mecklenburg-Vorpommern on 20 July 2023 under IMI 539360 within the informal consultation that it did not oppose the new draft decision.

8. The State Commissioner for Data Protection and Freedom of Information Mecklenburg-Vorpommern subsequently issued on 24 July 2023 under IMI 541190 a decision pursuant to Article 60(3) of the GDPR.

9. By decision of 2 August 2023, the Data Protection Authority removed the suspension in the proceedings at issue and granted the complainants the right to be heard.

10. The complainants responded by letter of 8 August 2023 and argued in summary that they could not understand the decision of the lead supervisory authority, as the respondent’s statements were untrue and unexplainable. The complainants felt that the lead supervisory authority had put itself very much on the side of the respondent.

B. Subject matter of the complaint

Based on the appellants’ arguments, the subject matter of the proceedings is whether the respondent disclosed personal data of the complainants to third parties and thereby violated general principles and the lawfulness of data processing pursuant to Articles 5 and 6 GDPR.

C. Findings

The data protection authority bases its findings on the procedure set out and documented under point A. and the findings of the lead supervisory authorities. It is apparent from the findings of the lead supervisory authority that the respondent did not disclose any personal data of the complainants to third parties.

Assessment of evidence: *The findings made are based on the present case file. The finding that the respondent did not disclose the complainant’s personal data to third parties is based on the findings of the State Commissioner for Data Protection and Freedom of Information Mecklenburg-Vorpommern as the lead supervisory authority. In summary, the disclosure of data attributed to the respondent by the appellants shows a diluted factual substrate as a whole, since the appellants merely rely on general external indicia (e.g. “blocking” of Facebook content by [REDACTED]) as well as to undated text messages from [REDACTED], from which it is not clear, however, that [REDACTED] had received data about the complainants from the respondent. Rather, the opposite is claimed there,*

namely that [REDACTED] has received the information about the complainants not by the respondent, but “by detours”, which does not appear impossible according general life experience. As will be shown in the legal analysis below, although no absolute certainty is needed for the assumption of a fact, it is necessary to have a certain (minimum) level of proof, which was not achieved in the present case by the complainants’ arguments.

D. Legal analysis

D.1. The “one-stop-shop” procedure

In accordance with Article 56(1) of the GDPR, without prejudice to Article 55 leg. cit., the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor.

In this way, the so-called “one-stop-shop” principle is introduced in cases of cross-border processing of personal data. It is intended to ensure a coherent application of the GDPR in cross-border data processing (see Peuker in Sydow [eds.], European General Data Protection Regulation, Art. 56 Rz 1).

In order to prevent conflicts of jurisdiction, Art. 56 GDPR stipulates that according to the criteria listed therein, one of the supervisory authorities concerned becomes the lead supervisory authority. In principle, it is responsible for the coordination of the conduct of the proceedings and the adoption of procedural or draft decisions.

In accordance with Article 56(1) of the GDPR, the local jurisdiction of the lead supervisory authority depends on the main establishment of the controller. Since, in the present case, the respondent is domiciled in the Federal Republic of Germany, Mecklenburg-Vorpommern, the Land Commissioner for Data Protection and Freedom of Information Mecklenburg-Vorpommern is competent.

D.2. The binding effect of procedural decisions of the lead supervisory authority

Pursuant to Article 60(1) of the GDPR, the lead supervisory authority shall cooperate with the other supervisory authorities concerned and endeavour to reach consensus.

In accordance with Article 60(3) of the GDPR, the lead supervisory authority shall immediately provide the supervisory authorities concerned with relevant information, submit the draft decision to them for comments and take due account of their positions.

Pursuant to Article 60(4) of the GDPR, the supervisory authorities concerned have the opportunity to object to it within four weeks of receipt of the draft decision.

If the lead supervisory authority joins the objection – as in the present case – it shall transmit a new decision (draft) to the supervisory authorities concerned in accordance with Article 60(5) of the GDPR, which in turn have the opportunity to comment on it within a period of two weeks. If no further objection is lodged within the deadline, the decision of the lead supervisory authority shall become binding on the

supervisory authorities concerned in accordance with Article 60(6) of the GDPR.

In the present case, in the absence of a (new) objection the Austrian Data Protection Authority is bound by the decision of the State Commissioner for Data Protection and Freedom of Information Mecklenburg-Vorpommern dated 24 July 2023.

In this regard, it should be noted that an objection made according to Article 60(4) of the GDPR may (also) serve the interests of the complaining party, nevertheless it primarily pursues the purpose of ensuring an objectively uniform application of law, detached from the individual interest of the parties (see Recital 135 GDPR and the possibility of initiating the consistency mechanism in accordance with Article 60(4) in conjunction with Article 63 et seq. GDPR). Similarly, the data protection authority is not competent for representing the complainants as a party representative in the proceedings.

D.3. On the adoption and service of the order giving effect to proceedings

Depending on its content, the adoption and notification of the decision are governed differently:

In the case of decisions which are fully granted, the lead supervisory authority shall adopt the decision, notify it to the controller in accordance with Article 60(7) of the GDPR and inform the other supervisory authorities concerned and the committee thereof. The supervisory authority to which a complaint has been lodged shall inform the complaining party of the decision.

In the case of dismissing decisions (or in case of rejection), in accordance with Article 60(8) GDPR, in derogation from paragraph 7 leg. cit., the supervisory authority to which the complaint was lodged (here: the Data Protection Authority), shall adopt the decision and notify it to the complaining party.

Finally, Article 60(9) of the GDPR provides for shared jurisdiction in cases in which the complaint is partially rejected or dismissed.

Since, in the present case, the decision of the lead supervisory authority constitutes a rejection of the complaint, the Austrian Data Protection Authority must adopt the procedural decision against the complainants in accordance with Article 60(8) GDPR. This ensures effective legal protection, as the complainants may contest the decision in the Member State in which they lodged their complaint.

D.4. In the matter

In accordance with Article 2(1) GDPR, the GDPR applies to the wholly or partially automated processing of personal data as well as for the non-automated processing of personal data stored or intended to be stored in a file system.

In accordance with Article 4(2) of the GDPR, the processing of personal data includes, *inter alia*, the reading, consultation, use, disclosure by transmission, dissemination or any other form of provision, provided that these are within the scope of the GDPR. The respondent is, without doubt, the controller within the meaning of the law. Article 4(7) GDPR for the processing of personal data of her customers.

In the present case, the alleged transfer of personal data of the appellants by the respondent to uninvolved third parties is criticized. External circumstances such as the blocking of Facebook content as well as undated text messages from [REDACTED] are raised as evidence. [REDACTED]

[REDACTED] states that she has not received such data from the respondent and also does not mention any details that may have led to her message.

In addition, the respondent's comments obtained by the lead supervisory authority do not show sufficient evidence that the complainants' personal data have been transmitted to [REDACTED] and are or should be stored in a file system. Even if the respondent had mentioned the names of the complainants in a telephone exchange with her acquaintance [REDACTED] regarding the handling of legal disputes, for the reasons mentioned above, it cannot necessarily be assumed that the scope of application of the GDPR would have been opened.

In this regard, it should be noted that an oral disclosure of personal data does not fall within the scope of the GDPR (see, for example, *Heißl* in *Knyrim* [eds.], DatKomm, Art. 2 GDPR para 55; as well as *Bergauer* in *Jahnel* [eds.], Comment on the General Data Protection Regulation, Art. 2 GDPR, paragraph 18).

In contrast, the (national) constitutional right to confidentiality under § 1(1) DSG does not require processing in a data application or manual file and therefore also protects, for example, the use of data in conventional or oral form (see the decision of the Austrian Data Protection Authority of 25 May 2020, Case No. 2020-0.191.240). However, the present case must be assessed solely on the basis of the GDPR (and not on the basis of § 1 DSG) due to its cross-border nature.

There is also insufficient evidence on the possible transfer of the complainants' personal data to other third parties from which such disclosure could be inferred.

As a result, the respondent's breach is neither plausible nor can it be proved. In this context, it should be noted that all the facts on which an official decision is to be based, generally require evidence. Unless otherwise provided by law, full proof of a fact must be provided. This means that the authority must obtain certainty as to the existence of the factual elements relevant to the decision (i.e. about a factual transaction, for example).

In the present case, the necessary evidence for a finding in this respect (see § 45(2) of the AVG) is not reached by the complainants' mere argument that the respondent has disclosed their personal data to third parties. That argument alone cannot give rise to an outstanding likelihood of the respondent's actual disclosure of personal data by the respondent, especially since the respondent and the third party dispute such disclosure.

Since no disclosure of their personal data alleged by the complainants could be established, it must be assumed that there is no such fact (see the ruling of the Austrian Supreme Administrative Court of 16 June 1992, Case No. 92/08/0062).

The appeal was therefore to be dismissed.

The Data Protection Authority does not overlook the recent ruling of the Austrian Supreme Administrative Court (see Austrian Supreme Administrative Court, 10.3.2023, Case No. Ra 2020/04/0085-9), according to which, in the case of disputed written statements, the credibility of persons may be examined in the context of an oral hearing. In the present case, however, it should be noted that the investigation procedure is not led by the Austrian Data Protection Authority, but by the lead supervisory authority within the meaning of the present case. Art. 56 in conjunction with Art. 60 of the GDPR and it is therefore solely due to the lead authority to adopt the investigative measures required by its national procedural law.

If the complainants raise a possible damage to their reputation or credit within the meaning of § 1330 Austrian Civil Code or within the meaning of evil impeachment according to § 111 Austrian Criminal Code, it should be pointed out that neither the lead supervisory authority nor the Austrian Data Protection Authority are competent to handle such reproach, but the ordinary civil or criminal courts.

EXPLANATION ON RIGHTS TO APPEAL

A complaint against this decision may be lodged in writing to the Federal Administrative Court within **four weeks** of notification. The complaint must **be lodged with the data protection authority** and must contain:

- the name of the contested decision (GZ, subject)
- the name of the competent authority,
- the grounds on which the allegation of illegality is based,
- the desire and
- the information necessary to assess whether the complaint has been submitted in good time.

The data protection authority has the possibility to amend its decision within two months either by **pre-trial decision** or to **submit the complaint with the file of the proceedings to the Federal Administrative Court.**

The complaint against this decision is subject to **a fee**. The fixed fee for a corresponding input including inserts is **EUR 30**. The fee must be paid to the account of the Austrian Tax Office, stating the intended purpose.

In principle, the fee must be transferred electronically with the function "Tax Office payment". The tax office Austria – Department of Special Competences should be specified or selected as the beneficiary (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). Furthermore, they are Tax number/delivery account number 10 999/9102, the tax type "EEE Complaint Fee", the date of the decision as the period and the amount.

If the e-banking system of your credit institution does not have the function “Tax Office payment”, the eps procedure can be used in FinanzOnline. An electronic transfer can only be excluded if no e-banking system has been used so far (even if the taxpayer has an internet connection). Then the payment must be made by means of a payment order, whereby attention must be paid to the correct assignment. Further information can be found at the tax office and in the manual *“Electronic payment and reporting on the payment of self-assessment duties”*.

The payment of **the fee** shall be **proved** upon submission of the complaint **to the data protection authority** by means of a payment document to be connected to the input or a printout of the issue of a payment order. If the fee is not paid or not paid in full, a **report shall be made to the competent tax office**.

A complaint lodged in good time and admissible to the Federal Administrative Court has **suspensive effect**. The suspensive effect may have been excluded in the sentence of the notice or may be excluded by a separate decision.

9 August 2023

For the Head of the Data Protection Authority:

[REDACTED]

GZ: D084.2680
2023-0.417.694

Case handler: [REDACTED]
[REDACTED]

Notification of personal data breaches to the supervisory authority (Art. 33 GDPR, "Data Breach Procedure")

[REDACTED] (A56ID 290800)

FINAL DECISION

Subject: Discontinuation of the procedure

By notification dated 17 March 2021 and subsequent notifications dated 25 March 2021 and 4 May 2021, [REDACTED], [REDACTED] and [REDACTED] (controllers), represented by [REDACTED], informed the AT DPA that they were reporting a personal data breach.

[REDACTED] is the parent company of the two Austrian subsidiaries [REDACTED] and [REDACTED]. [REDACTED] operates the entire IT landscape.

In summary, a **ransomware attack** occurred on 15 March 2021 at [REDACTED], [REDACTED], [REDACTED] and [REDACTED]. The attacker abused an MS Exchange vulnerability. The incident led to an **encryption of data**. The company [REDACTED] was commissioned with a forensic investigation of the incident.

In total, about 3,000 suppliers (B2B contacts) and about 250 employees were affected by the incident.

Regarding the suppliers, data of the categories

- Name
- Address
- Telephone number
- E-mail address
- Bank details

and regarding employees, data of the categories

- Name
- Address
- Telephone

- E-mail address
- Bank details
- Health insurance number
- Application documents
- Proof of citizenship
- Passport
- Registration form
- Birth certificate
- Proof of education
- Marital status
- Degree of disability, if applicable
- Religious Confession

were affected.

The forensic investigations have shown that neither personal data were stolen nor unauthorized persons had access to personal data. There was no particular ‘traffic’ on [REDACTED]’s data line during and after the attack, which is why it could be assumed that no data had been stolen.

The controller has taken the following measures to remedy the injury or mitigate possible adverse effects:

- Forensic investigation
- Information to the affected employees of [REDACTED] and [REDACTED]
- Implementation of patches with regard to the vulnerability
- External back-ups

The controller has taken appropriate steps to minimize the risk and to eliminate, as far as possible, the adverse consequences of the security breach. Further measures of the Data Protection Authority as of Art. 58(2)(e) GDPR (order the controller to communicate a personal data breach to the data subject) or § 22(4) DSG (order in case of risk) are not required.

The procedure is therefore terminated and this is finally brought to the attention of the controller.

7 August 2023

For the Head of the Data Protection Authority:
[REDACTED]

**Litigation chamber****Decision 2019/ [number] of 15 May 2019**

File number: [REDACTED]

The Litigation chamber of the Data Protection Authority, composed of [REDACTED] President, and [REDACTED] members;

Considering the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC* (General data protection regulation, hereafter GDPR);

Considering the Act of 3 December 2017 *establishing the Data Protection Authority*;

Considering the rules of procedure as approved by the Chamber of Representatives on 20 December 2018 and published in the *Belgian Official Journal* on 15 January 2019;

Considering the documents from the file;

decided as follows concerning:

- the complainant: [REDACTED]
- the controller: [REDACTED]

1. Facts and procedure

On the basis of Article 95, §2 of the Act of 3 December 2017 establishing the Data Protection Authority, the Litigation chamber informs you that a file is pending as a result of the complaint.

The complaint concerns the failure of [REDACTED] to comply with [REDACTED]'s request to exercise her right of access. In the framework of her son's studies, a contract has been concluded with the controller, which was at that time [REDACTED], for the rental of a studio. For the purpose of the guarantee, a copy of the identity card as well as data on the complainant's income were provided to that same controller. When it was reported to her son that [REDACTED] would now be the controller, the complainant asked to access her personal data. She was then informed by [REDACTED] that they didn't have any personal data about her and that the information which had been transmitted to [REDACTED] should have been erased. The complainant argued that this was not possible as the contract was still in force. The complainant urged again [REDACTED] to provide her access to her personal data.

2. Legal basis

Art. 15 GDPR:

1. *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*
 - (a) *the purposes of the processing;*
 - (b) *the categories of personal data concerned;*
 - (c) *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
 - (d) *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
 - (e) *the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; f) the right to lodge a complaint with a supervisory authority; g) where the personal data are not collected from the data subject, any available information as to their source;*

- h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*
2. *Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.*
 3. *The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*
 4. *The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.*

3. Justification

Despite the complainant's query to [REDACTED] to comply with her request to exercise her right to access, the controller failed to react adequately.

It follows from that finding that an infringement of the abovementioned provision must be regarded as proven.

FOR THESE REASONS,

The Litigation chamber of the Data Protection Authority decides, after deliberation, as follows:

- pursuant to Article 58.2. c) of the General Data Protection Regulation (hereafter GDPR) and Article 95, §1, 5° of the aforementioned Act of 3 December 2017, the Litigation chamber decides to order the controller to **comply with the data subject's requests to exercise her rights, more specifically her right of access** (Article 15 of the GDPR).
- pursuant to Article 95, §1, 8° of the Act of 3 December 2017, **to publish that decision on the website** of the Data Protection Authority, albeit after anonymisation.

In application of Article 60.10. of the GDPR, attention is drawn to the fact that the controller is bound to notify to the Data Protection Authority the measures he has taken to ensure compliance with the

decision. Pursuant to Article 12.3 of the GDPR, the controller shall provide information on the action taken on the decision to the Litigation chamber within one month of receipt of this decision.

This decision can be appealed to the Market Court within a period of thirty days starting from the service of the notification (Article 108, §1 of aforementioned Act of 3 December 2017).

If the controller wishes to make use of the possibility of consulting and copying the file (Article 95, §2, 3º of the Act of 3 December 2017), he should contact the secretariat of the Litigation chamber in order to make an appointment.

If a copy of the file is requested, the documents shall be sent by ordinary mail unless the controller wants to pick them up on the spot at the secretariat of the Litigation chamber.

President of the Litigation chamber



Litigation Chamber

Decision 02/ 2019 of 15 May 2019

File number: DOS-2019-01171

Subject: Cross-border complaint for non-compliance by the controller with a request to exercise the right to erasure

The Litigation Chamber of the Data Protection Authority, composed of [REDACTED] president, and [REDACTED] and [REDACTED] members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), hereinafter GDPR;

Having regard to the Law of 3 December 2017 *establishing the Data Protection Authority*;

Having regard to the internal rules of procedure as approved by the House of Representatives on 20 December 2018 and published in the *Belgian Official Gazette* on 15 January 2019;

Having regard to the documents in the file;

has decided as follows in the matter of:

- the plaintiff: [REDACTED]
- the controller: [REDACTED]

1. Facts and procedure

On the basis of Article 95, §2 of the Law of 3 December 2017 *establishing the Data Protection Authority*, the Litigation Chamber informs the controller of the fact that a file is pending as a result of the complaint.

The complaint concerns the non-compliance of [REDACTED] with the request by [REDACTED] [REDACTED] to exercise his right to erasure ("the right to be forgotten"). He filled in the web form twice in order to excercise his right to erasure and received no answer. He also sent an email with the same request on 28 June 2018 to [REDACTED], as well as to [REDACTED], asking to have his data erased. Nor to this did the data subject receive any answer, although Article 12.3. of the General Data Protection Regulation provides for the controller to inform the data subject about action taken on the request, without undue delay and in any event within one month of receipt of the request. If needed that period may be extended by another two months, depending on the complexity and number of the requests.

2. Legal basis

- Article 12.3. General Data Protection Regulation

"The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject."

- Article 17. General Data Protection Regulation

"1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: a) for exercising the right of freedom of expression and information; b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or e) for the establishment, exercise or defence of legal claims."

3. Justification

Despite the plaintiff repeatedly asking [REDACTED] to comply with his request to exercise his right to erasure, the controller did not respond. It appears clearly from the facts that the deadline for responding to the plaintiff's request has been exceeded in every respect.

As a result of these findings an infringement of the aforementioned provisions must be regarded as proven.

ON THESE GROUNDS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation:

- by virtue of Article 58.2. c) of the GDPR and Article 95, §1, 5° of the Law of 3 December 2017, **to order the controller to comply with the plaintiff's requests to exercise his rights, in particular the right to erasure ("the right to be forgotten")** (Article 17 of the GDPR);
- by virtue of Article 95, §1, 8° of the Law of 3 December 2017, **to publish that decision on the website** of the Data Protection Authority, albeit after anonymisation.

In application of Article 60.10. of the GDPR, attention is drawn to the fact that the controller is required to communicate the measures he has taken to comply with the decision to the Data Protection Authority. Having regard to Article 12.3. of the GDPR, the controller shall provide information on action taken on the decision to the Litigation Chamber within one month of receipt of this decision.

This decision may be appealed within thirty days after service of the notice¹ at the Markets Court² (Article 108, §1 of the aforementioned Law of 3 December 2017).

If the controller wishes to make use of the possibility of consulting and copying the file (Article 95, §2, 3° of the Law of 3 December 2017), he should contact the secretariat of the Litigation Chamber in order to make an appointment.

If a copy of the file is requested, the documents shall be sent by ordinary mail, unless the controller wishes to pick them up at the premises of the secretariat of the Litigation Chamber.

(signed) [REDACTED]
[REDACTED]

¹ The date of this letter shall serve as the date of service of the notice.

² Court of Appeal of Brussels.



Autorité de protection des données

Litigation Chamber

To the attention of

[REDACTED]

Secretariat

T: +32 (0)2 274 48 57

F: +32 (0)2 274 48 35

E-mail: litigationchamber@apd-gba.be

Your reference

Our reference

Enclosure(s)

Date

DOS-2019-03838

Subject: Complaint against [REDACTED]

Dear Sir,

During its session of 23 July 2019, the Litigation Chamber decided to refer to the Inspection Service the complaint that you had lodged with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) against [REDACTED] in its capacity as lead authority in this matter.

On 6 December 2019, the Inspection Service communicated its report to the Litigation Chamber. Enclosed you will find a copy of this report. Under the terms of this report, the Inspection Service notes from the complaint:

"Finding 2: except information (result pages) obtained on search engines and information processed by third parties, no public or operational processing activity by the controller [REDACTED]
[REDACTED] can be found. The website [REDACTED] no longer appears to be active or accessible to users."

On the basis of these findings, in application of article 95, §1 and 3° of the Act of 3 December 2017 establishing the Data Protection Authority, the Litigation Chamber decides to dismiss your complaint without follow-up since with the liquidation of [REDACTED] it is no longer possible to deal with the complaint.

...



Yours sincerely,



President of the Litigation Chamber

Summary Final Decision Art 60

Complaint

Dismissal of the case

EDPBI:BE:OSS:D:2020:96

Background information

Date of final decision: 20 March 2020

LSA: BE

CSAs: NL, SE

Legal Reference: Right to erasure (Article 17)

Decision: Case dismissed following controller's liquidation

Key words: Right to erasure, Liquidation

Summary of the Decision

Origin of the case

The complainant requested to have his data removed but received no answer from the controller.

Findings

The LSA issued a report on the matter, which concluded that the controller's website was no longer active or accessible to users. Result pages obtained on search engines and information processed by third parties were the only sources of information that could be located. No public or operational processing activity by the controller could be determined.

Decision

This complaint was dismissed without follow up as it is not possible to contact the controller due to its liquidation.

Summary Final Decision Art 60

Own volition

Administrative fine

EDPBI:BE:OSS:D:2020:200

Background information

Date of final decision:	14 May 2020
Date of broadcast:	02 April 2021
LSA:	BE
CSAs:	AT, CY, DE-BB, DE-BE, DE-BW, DE-BY, DE-NI, DE-NW, DE-RP, DK, ES, FR, HU, IE, IT, LV, NL, NO, PT, SE, SI, SK.
Legal Reference(s):	Lawfulness of processing (Article 6), Consent (Article 7)
Decision:	Administrative fine
Key words:	Social media, Lawfulness of processing, Consent, Legitimate interest

Summary of the Decision

Origin of the case

As part of an own volition enquiry, the LSA assessed the compliance of a social media platform in relation to processing of contact information relating to members and non-members of the platform for the purposes of sending invitations.

In this regard, the LSA found that the social media platform collected and stored non-user contact details on its servers after requesting from its existing users the permission to access their contacts' address book, which included name, phone numbers and "other information on third-party platforms". The non-users' contact details were then used by the social media platform to send invitation messages to these non-users via the member-user's profile.

As regards the procedure for sending emails to existing members, the LSA noted that the list of recipients for sending these invitations was pre-ticked by default.

In addition, the social media platform retained the personal data for a period of three months after closure of the account by the users, unless a user decided to end the synchronization of its contacts.

Findings

Firstly, the LSA found that the so-called “household exemption” did not apply to the storage of contact details by the platform and the sending of invitations in the name and on behalf of the platform, considering that the social media platform controlled both the means and purposes of this processing.

Regarding the legal basis for the collection of non-users’ personal data, the LSA found that this processing could not rely on the legal basis of the consent as users giving access to their contact list cannot give valid consent on behalf of non-users. The LSA also considered that whereas the controller could not legally invoke a “legitimate interest” as a legal basis for this processing, contact details of non-users can however be used to check whether or not they are already members of the platform (“compare and forget” action), under the condition that appropriate technical and organisational measures are implemented.

As to the processing relating to the sending of invitation emails to non-users, the LSA also considered, in light of the circumstances of the processing, that neither consent of non-users, nor the legitimate interest of the controller could apply as legal basis.

Concerning the processing relating to the sending of invitation emails to existing users, the LSA concluded that this processing could not rely on a valid consent to the extent that the list of recipients was pre-ticked. However, the LSA stressed that this processing was not necessarily unlawful as it may rely on the legal basis under Article 6.1.b GDPR or Article 6.1.f GDPR, depending on the circumstances of the processing. In this respect, the LSA pointed out that pre-ticked lists of recipients would be also problematic in case of reliance on one of these legal bases.

Decision

The LSA imposed an administrative fine of 50,000 euros to the controller for the unlawful processing of non-users’ personal data, as well as for the processing of existing users’ personal data during the period when the list of recipients of invitation emails were pre-ticked in advance.



Litigation Chamber (Geschillenkamer)

Decision on the merits 25/2020 of May 14th 2020

File number : DOS-2019-01156

Subject: Legal basis for the processing of personal data by a social media platform

The Litigation Chamber of the Data Protection Authority, composed of [REDACTED]

[REDACTED] members;

Having regard to Council Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on *the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC* (General Data Protection Regulation), hereinafter GDPR;

In view of the Act of 3 December 2017 *establishing the Data Protection Authority*, hereinafter DPA Act;

Having regard to the internal rules, as approved by the House of Representatives on December 20, 2018 and published in the Belgian Official Gazette (Belgisch Staatsblad) on 15 January 2019;

Having regard to the documents in the file;

has taken the following decision on:

- processing of personal data by the controller: Y ("defendant");

1. Facts and procedure

2. On November 28, 2018 the Executive Committee of the Belgian Data Protection Authority (DPA) decided to initiate a case by its Inspection Service on the basis of Article 63, 1 ° of the DPA Act. The reason for the aforementioned referral was the practice of the social network website "W" of inviting "*friends/contacts*" of those members.
3. The Inspection Service informed the defendant about the decision of the Executive Committee in a letter dated 12 March 2019.
4. The Inspection Service sent the defendant two letters dated March 12, 2019 and May 16, 2019, with questions concerning alleged infringements of Articles 5, 6, 7, 30, 37 and 38 of the GDPR. More specifically, the Inspection Service asked questions regarding the categories of personal data of non-users which have been gathered and the retention of such data; an extract from the record of processing activities of the defendant and questions concerning the Data Protection Officer (place in the organization, activities, professional qualities, commitment to responding to the questions of the Inspection Service).
5. The defendant replied to the questions of the Inspection Service by letters dated 12 March 2019, 3 April 2019 and 14 June 2019. The defendant explained as follows the processing of personal data of the invitation functionality "W" website: "*Any personal information that we collect will depend on the platform used, if a user chooses to upload contacts from the phone book of his or her cell phone, we will collect telephone numbers and names that the user attaches to the phone. If a user chooses to upload contacts from their e-mail account, the basic contact information uploaded will be determined by the own e-mail provider of the user, as clearly set out in the upload permission screen from this provider*".¹ If a user chooses to upload his or her contacts from his/her phone these contacts are synchronized correctly, so that the user can invite the new people who are not members of "W" to register.
6. The defendant explained that in addition to the consent button, this paragraph with information is displayed: "*On a regular basis we will import contacts and save them, so we can notify you when registering acquaintances in "W" and can invite them to register you when your contacts are not yet members of "W". You decide who you add. You can stop the import at any time and delete all contacts. More Information*".

¹ Letter from the defendant dated 14 June 2019.

7. When the user clicks on "more information", he or she will see the following additional information:
*"When you import your address book we will periodically import information on your contacts, such as names, phone numbers and other information as illustrated on the consent screen of the provider to our servers. We use this information to inform you about who you already know on W and then you can invite your contacts who are not yet members. The aforementioned suggestions are made directly to the service and through e-mail. We cannot store your password or e-mail anyone without your consent. You can stop synchronising your address book at any time via your settings. When you do this, it will delete all previously imported contacts. For more information on how we handle your personal information we refer to our Privacy Policy."*².
8. The defendant further explains that the contacts of the user in the database of the defendant are kept until the user decides to stop synchronizing his contacts, or if a user deletes specific contacts. When an account is closed, the contacts (either consciously or after two years of inactivity) are removed within three months, the defendant explains³.
9. In his letter of 9 March 2020, the defendant explains that the user can choose to withdraw his consent and no longer have his contacts synchronized, with the result that existing contacts will be deleted from the "W" database. In case the user does not choose this option, the contact details (including those of non-users of the website) will be retained for a minimum of three months⁴.
10. The defendant remitted an extract from the record of processing activities to the Inspection Service showing the categories of personal data about customers (users of the website) that are processed "*profile information, personal identification, analytical data, user generated content, user account information, contact information and third party information (for users who register via Facebook)*". According to the record, the invoked legal basis for processing is "*the execution of a contract*" and "*consent of the data subject*"⁵.
11. Regarding the legal basis for the collection of non-users' personal data, the defendant explained as follows that the legal basis of "*consent*" - in his opinion - should not have been used: "*We believe that we are not obliged to collect the contact person's consent. Indeed, we do not send promotional messages because it is the user who sends personal communication to his or her contact through our platform. This interpretation is in line with the vision set put in Opinion 5/2009*

² Ibid.

³ Ibid.

⁴ See also Art. 11 of the defendant's Privacy policy, exhibit 5 of the Inspection report.

⁵ Ibid.

of the Working Party 29 Working Party on online social networking⁶ and we have ensured that our process is fully in line with the four criteria set forth in [the] opinion ".⁷⁸

12. In his letter dated 14 June 2019, the defendant replied in detail to the questions of the Inspection Service regarding the activities and competence of its data protection officer⁹. The defendant referred inter alia to the professional experience of the person, in particular his experience as ██████████ at a company engaged in online payments and as lawyer at the IT department of a law firm. This person also holds an ██████████¹⁰ certification.
13. On 18 June 2019, the Inspection Service remitted its report to the Litigation Chamber, under Article 92, 3° of the DPA Act.
14. The inspection report identifies potential infringements of art. 5, paragraph. 2 of the GDPR, of Article 6 of the GDPR, items 4, 11), and 7 of the GDPR, as well as of articles 37 and 38 of the GDPR.
15. Concerning the alleged breaches of accountability (art. 5, paragraph. 2 of the GDPR), the lawfulness of processing (Article 6 of the GDPR), and the definition of and conditions for authorization (Articles 4, 11) and 7 of the GDPR), the inspection report makes a distinction between, on the one hand, the consent of the personal data of the user of the website and, on the other hand, the consent relating to the personal data of the contacts of the user.
16. Regarding the argument of the defendant that he is not required to collect *consent of the contacts (non-members of "W")*, since it would involve "*personal communication*" by the user, the Inspection Service notes that the exception for personal or household activities can indeed be invoked by social media users, but not by the social network "*W*" itself, in accordance with paragraph 18 of the GDPR which reads as follows: "*personal or household activities [outside the scope of GDPR] may include [...] social networks and online activities in the context of such activities. This Regulation does apply to controllers or processors who provide the means for processing personal data for such personal or household activity*" (Inspection Report, p. 4).

⁶ Opinion 5/2009 of Group 29 on social networks, 12 June 2009 (WP 163). All Group 29 and EDPB quoted in this decision are available via www.edpb.europa.eu.

⁷ Letter to the Inspection Service dated April 3, 2019.

⁸ Letter from the defendant dd. 14 June 2019.

⁹ Letter from the defendant dd. 14 June 2019.

¹⁰IAPP is a globally recognized private organization that offers certifications on European data protection law (CIPP/E) and data protection management (CIPP/M), see the following web page: <https://iapp.org/certify/cippe/>

17. The reference by the defendant to Opinion 5/2009 on online social networking of the Working Party 29 of 6/12/2009 is not considered relevant by the Inspection Service, since that opinion relates to the former Data Protection Directive¹¹ and "*because the GDPR imposes more extensive obligations on controllers, including the accountability of Article 5, paragraph 2 of the GDPR and the requirements of an unambiguous indication in Article 4, 11) and Article 7 of the GDPR*" (Inspection Report, p. 5).
18. Regarding the *consent by the social media users (members of "W")*, the Inspection Service notes that there are options previously ticked in the procedure of adding contacts. Therefore, the consent of the user whether or not to use the personal contacts is not considered valid in a context where Recital 32 of the GDPR explicitly clarified that "*pre-ticked boxes*" do not constitute consent. The Inspection Service notes that the defendant is willing to "*cease his practice on the basis of which he contacts pre-selected persons*", which has now happened (two working days after the receipt of the inspection report)¹².
19. The defendant has meanwhile removed previously ticked options from the platform "*voluntarily and without any disadvantageous acknowledgment*" from the platform, upon receipt of the second letter of the Inspection Service dated May 16, 2019. The defendant, however, alleges in his conclusion that the pre-ticked options are not related to obtaining the consent of the user to import contacts, and, moreover, this does not require consent, taking into account the principles of the Opinion 5/2009 of Working Party 29 on online social networking (see the conclusion of the defendant, p. 13).
20. The Inspection Service also noted that it is not indicated in relevant privacy information that consent may be withdrawn, as required by Article 7 GDPR. In his conclusion (p. 19 and 20) and in his letter of 14 June, the defendant replied that the possibility to withdraw the consent is indeed available on the website. Users are informed that they can stop the import at any time and delete all contacts.
21. Before starting this procedure, the defendant had been in contact with the GDPA after a previous complaint received concerning the method used on the "*W*" platform. The complaint was on the fact that the information relating to privacy could only be read only after creation of an account and after accepting the terms of use and privacy policy. The DPA had informed "*W*" that this was

¹¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Pb L 281/31 ("Data Protection Directive").

¹² Conclusion of the defendant, p. 13 and 42.

not a valid way to obtain consent for the “*invite a friend*” e-mail; consent was the legal basis used by “W” for the processing of user data.¹³

22. During the hearing on 9 July 9 2019, the Litigation Chamber decided under Article 98 of the DPA Act that the file was ready for handling on the merits.
23. On 10 July 2019 the defendant was informed of this decision by registered letter, and was also given the inspection report, and the inventory of the documents on the file which had been transferred to the Litigation Chamber by the Inspection Service. In addition, the defendant was informed of the provisions mentioned in Article 98 of the DPA Act and the defendant was, based on Article 99 of the DPA Act, informed of the deadlines to submit his defence. The deadline for receipt of the briefs (“conclusion”) of the defendant was established on 4 September 2019.
24. By letter and e-mail on 15 July 2019 the defendant asked to be heard. The Litigation Chamber informed the defendant of the date of the hearing by letter dated 30 August 2019.
25. On 4 September 2019, the Litigation Chamber received the defence conclusion of the defendant
26. On 1 October 2019, the hearing took place. The file was retaken with other members of the Litigation Chamber. The controller was heard and was given the opportunity to put forward his arguments in response to the questions put to him by members of the Litigation Chamber, regarding the foreign reach of the “W” website, the legal basis for the processing of personal data of users and non-users of the “W” website and the role and working methods of the data protection officer.
27. During the hearing, the defendant made the following statements that confirm and/or complement its conclusion:
 - The defendant provides a platform so new people meet in private without limitation (friend or relation); there are 4.5 million active users per month across the world, with 1.5 million users in the EU. It employs 33 people at “W” and 100 people in various places in the world for the helpdesk (no employees of Y, but only contractual services).
 - The defendant complains that the constitutive components of the alleged “offense” are not disclosed to “W” in the inspection report (see also conclusion of the defendant, p. 6); the defendant finds that the indictment was issued in this case without a prior detailed account

¹³ Letter from the DPA to the defendant dated 7/03/2018

of the alleged infringement. The defendant believes that the allegations regarding the "*accountability*" is particularly unclear.

28. The defendant also explained how the invitation process takes place on the "*W*" site:¹⁴

- The website users are informed about the processing taking place in the context of the "*invite a friend*" feature.
- Under the message "*W is better with friends*", the Internet user has the possibility to import an address book from various service providers (Outlook, Google Mail, Yahoo, Facebook, Telenet, Skynet). The user is not required to select a service provider and can skip the "*invite a friend*" feature completely. If the user wants to make use of this feature he must select one of the service providers. Then a screen is shown from this service provider, by which the Internet user can allow his contact addresses to be read. This is, as explained by the defendant, "*the permission screen is of the service provider.*" If the internet user agrees, all addresses stored in the address book then are stored by "*W*". The feature offered by such service consists in allowing users to give limited contact information to share with the "*W*" platform for limited purposes.
- In a next step, the internet user gets the possibility to select the recipients of the invitations e-mails.
- A first version of the website had all addresses ticked, with the possibility to deselect all the recipients with one click. Addresses are no longer pre-ticked since 12 July 2019¹⁵, and the user has the choice between two options: designate the recipients one by one, or select all prior contacts with one click. In the previous version of the website, the user also had the opportunity to deselect pre-selected recipients one by one.
- In a letter dated 4 November 2019, the defendant insists that the users have the possibility to withdraw their consent for the use of the '*invite-a-friend feature*' at any time. The website announced that all previously imported contacts are then removed.

29. The defendant furthermore states that the details of the contacts can only be used for the invite feature. No profiles are prepared on the basis of this contact according to the defendant.

¹⁴ See also conclusion of defendant, p. 7-20.

¹⁵ Conclusion defendant, p. 13, nb. 28.

30. With regard to the alleged legal basis, the defendant alleges the following: when a user sends an invitation to his friends, it is a personal communication, not a marketing message which is subject to the anti-spam rules in the e-Privacy Directive; the defendant used only one legal basis, i.e. the consent of the users; *the "GDPR does not say that you do not need consent from contacts. We have the consent of the user, to import data,"* the defendant argued at the hearing. When asked by the Litigation Chamber whether the consent of the user according to the defendant is valid also for non-users of the "*W*" website, the defendant replied positively, "*since it regards one and the same purpose*" of processing. The defendant thus confirmed the positions taken in its conclusion, and which was summarized as follows by the defendant:

"With regard to the alleged legal basis, the defendant states the following: Y processes the contact details of the user for a single purpose: providing the "invite a friend" feature. To fulfil this sole purpose, the contacts of the user are uploaded and then invitation e-mails are sent on behalf of the user to the contacts that the user has selected. The legal basis on which Y relies for the processing of personal data under the "invite a friend" feature, is the consent of the user. Y is of the opinion that it is not required to distinguish the consent of the contacts from the user's request, since the processing of personal data is already justified by the consent of the user under Article 6 of the GDPR and as the invitation message sent on the other hand is not a direct marketing message subject to the ePrivacy Directive. This was explicitly confirmed by the Article 29 Working Party. When asked by the Litigation Chamber whether the consent of the user is valid for non-users of the "W" website, the defendant provides a positive answer: in the context of the 'invite a friend' feature and, more generally, of all services and functions that enable the users to process personal information of the contacts and other information from people they know (eg. e-mail services, messaging systems, operating systems, cloud services where people upload photos to show to their friends and family, ...), the data are in the first place of the user himself." (Letter of the defendant to the Litigation chamber of 4 November 2019, in response to the draft minutes of the hearing, p. 3).

31. The defendant then shows by using printed screens of the website that the user can see and edit the template before it is sent as part of the invitation e-mail (p. 12 of the hearing briefs). The defendant reiterates he feels he has taken all measures to ensure that this processing would meet the requirements of "*personal communication*" as set out in Opinion 5/2009 of the Article 29 Working Party on online social networking. According to the defendant, the Inspection Service falsely alleges that the opinion is no longer valid because it dates from before the entry into force of the GDPR and the consent requirements are since strengthened (see also conclusion, p. 23).

The defendant also discusses the question whether or not there is a marketing message within the meaning of Article 13 of the ePrivacy Directive. By letter dated 4 November 2019 the defendant gave further clarification: "*Y has never claimed that the GDPR would not apply to the processing operations carried out in the context of the W platform. Y is of the opinion that the invitation message transferred to the selected contacts of the user contains personal communication for which it is not required to obtain consent from such contacts according to the ePrivacy Directive.*"¹⁶

32. The Litigation Chamber then asks whether users in the invitation e-mail that the "W" platform gives are informed or not that their data may be corrected or deleted. The defendant refers to his hearing briefs that include a printed version of the screen to show what the recipient of such invitation sees: Under the message "*X. sent you a message*", two blue buttons offer the following option: "*Register and reply*" or "*Read-only message*". Under these buttons the following explanation appears: "*When you click on "Register and Sign", you agree to create an account for you on W and agree with our [hyperlink] Terms and Conditions. Please read our [hyperlink] Privacy Policy and our [hyperlink] Cookie Policy.*". The defendant explains that the recipient of the invitation e-mail obtains information on his rights through the Privacy and Cookie Policy of "W" and that the recipient also in the e-mail itself will get the following information: "*Click here if you do not want to receive commercial e-mails about our products or services*" (p. 17 of the hearing briefs).

33. With regard to the data protection officer, the defendant refers to documents showing that this person has been clearly involved in the definition of the invitation feature, including an e-mail of 13 August 2018 that has already been communicated to the Inspection Service (p. 15 of the hearing bundle). The defendant states that his data protection officer can report to the highest management, and that he actually does so according to the defendant (letter of the defendant to the Litigation Chamber dated 4 November 2019, p. 4). The defendant also argues that there is no evidence in the Inspection report that this person would not be independent (that he would receive instructions from the management, for example).

34. The defendant refers to a positive and recent assessment report demonstrating that the person does not have to fear for his job. According to the defendant, this positive assessment proves that the data protection officer is able to carry out his duties independently, and that V was the natural choice for a data protection officer. The data protection officer is based in Dublin but can communicate in English and French with the staff of the defendant, and there is also a local

¹⁶ Letter of the defendant to the Litigation Chamber dd. 4 November 2019, p. 4.

"privacy lead" in U. The defendant argues that the data protection officer meets the employees of Y regularly in person and that most meetings are via "video conferencing" software. The professional qualifications of the person emerge from his CV. The data protection officer states that he also works for another social media platform ("Z") and that there is no predetermined distribution with respect to its activities between the two platforms, and that he can rely on a team of four full-time employees in addition to the local privacy lead in U.

35. In view of the cross-border nature of the processing carried out by the defendant, the Litigation Chamber decided to launch the procedure of Art 56 GDPR, in order to identify the lead supervisory authority and the concerned supervisory authorities. The DPA claimed that it was the potential lead supervisory authority. The authorities from the following countries declared to be concerned authorities: The Netherlands, Germany (Lower Saxony, Baden-Württemberg, Brandenburg, Rhineland-Palatinate Mecklenburg-Western Pomerania, Bavaria, North Rhine Westphalia, Berlin), Portugal, Sweden, Ireland, Latvia, Italy, Norway, Hungary, Austria, Spain, France, Cyprus, Slovak Republic, Denmark, Slovenia.

36. On 3 October 2019, the Litigation Chamber sent a registered letter to the defendant with the financial statements of the defendant as attachment for the fiscal years 2018, 2017 and 2016, with the question whether the defendant could confirm the therein contained figures including turnover. The turnover figures are as follows:
 - year 2016: XXX EUR;
 - year 2017: XXX EUR;
 - year 2018: XXX EUR.

37. On 17 October 2019, the counsel for the defendant confirmed on behalf of the latter that the statements listed above are correct. Through this letter, the defendant wanted to draw the attention of the Litigation Chamber to an attached forecast for fiscal year 2019 (see below).

38. Minutes of the hearing were sent by e-mail for information purposes dated 30 October 2019 to the defendant, asking him to respond within 2 working days if he has any comments. The defendant was informed that this would not reopen the debates and that the comments should only relate to the display of the oral debates.

39. The defendant submitted his comments to the Litigation Chamber and urged, among other things, to take into account "*the fact that Y was always willing to cooperate since long before the official*

*start of the investigation and that the DPA was repeatedly asked for feedback which was never given.*¹⁷

40. On 5 November 5 2019 the matter was discussed again at a meeting of the Litigation Chamber. The Litigation Chamber concluded to initiate the cooperation procedure provided for in Article 60.3 GDPR.
41. An English translation of the draft decision was handed over to the concerned DPA on 8 January 2020, in line with Article 60.3 GDPR. The defendant was informed of this by letter dated 15 January 2020.
42. The Netherlands filed a relevant and reasoned objection on 4 February 2020. The Netherlands asked amongst other things to include more references to ECJ case law as regards the analysis of the defendant's legitimate interest to send invitation e-mails to third parties not using the social media platform. The Netherlands also challenged the relevance of a reference to an investigation report dated 2013 and which relates to the legitimate interest of social media platforms to send invitation e-mails.
43. The Litigation Chamber decided on 14 February 2020 to uphold the filed objection, in particular as regards the assertion that the application of the legal basis of legitimate interest *in the present case* requires an assessment in *concrete terms* of all relevant factual elements, taking into account the case law of the Court of Justice. The Litigation Chamber decided to reopen the debates as regards the analysis of the legitimate interest of the defendant.
44. The Litigation Chamber informed the defendant by registered letter of 18 February 2020 of this relevant and reasoned objection, as well as of its content, and invited the defendant to respond by 09 March 2020 at the latest regarding the possible invocation of legitimate interest as a legal basis for the disputed data processing operations. The defendant submitted its reply by letter of 09 March 2020.
45. The Litigation Chamber then took note of the defendant's arguments regarding their legitimate interest and, following the Inspection Report and taking into account the defendant's argumentation, ruled that it would impose a fine of €50,000 on the basis of the violations of the GDPR which it had established.
46. In order to give the defendant the opportunity to defend themselves on the amount of the fine proposed by the Litigation Chamber, the latter decided to list the relevant infringements in its

¹⁷ Letter from the defendant to the Litigation Chamber dated 4 November 2019, p. 1.

standard "form for reaction against the proposed fine", which was sent by e-mail of 7 April 2020, stating that the defendant was free to further complete this document with its reaction on the particular circumstances of the case, the proposed amount of the fine and the annual figures submitted¹⁸ The defendant replied by e-mail of 28 April 2020¹⁹ with its arguments concerning the amount of the fine as well as new information concerning the turnover for the fiscal year 2019, which exceeds €10,000,000 EUR according to the latest forecast of the defendant.

47. In the meantime, the Litigation Chamber decided to submit a revised draft decision to the relevant authorities on 23 April 2020 in accordance with Article 60.5 of the GDPR. This international procedure ended on 08 May 2020, without any reasoned objection.
48. The Litigation Chamber then adjusted its decision to take into account the defendant's arguments regarding the fine²⁰.

2. Decision

2.1 Qualification of the controller and of the processing

49. The defendant is the controller for the processing of the data of the users of the social media platform "W" and for the processing of the non-users' contact details (names, phone numbers or e-mail addresses) and other information of the contacts²¹ that are stored on the servers of "W" *in response to the synchronization of the address book (phone or e-mail) of the users of the website.*
50. Under Article 4.7 GDPR the controller is indeed "*a natural or legal person, public authority, agency or any other body, whether a third party or not, to whom/which the personal data are disclosed. [...]"*
51. The Court of Justice has at various occasions explained that the concept of 'controller' should be defined broadly as the natural or legal person, public authority, agency or any other body which

¹⁸ This invitation to submit limited submissions was sent by e-mail in the context where the Litigation Chamber was unable to accept this invitation to submit limited submissions by registered letter in accordance with Art. 95 LCA, and with the notification that if necessary the Litigation Chamber was prepared to grant longer periods to the defendant to lodge submissions (in the context of the Coronavirus outbreak). The defendant did indeed receive this e-mail and was able to respond within 3 weeks.

¹⁹ The defendant's arguments in this respect are discussed under the heading 'Decision regarding the penalty'.

²⁰ See the title "Decision concerning the penalty".

²¹ See the conclusion of the defendant, p. 11: "*This app wants consent to: See your Google contacts; Edit your Google contacts; Delete your Google Contacts; your contacts may include the names, phone numbers, addresses and other information about the people you know.*"

alone or jointly with others determines the purposes and means of the processing of personal data, with the aim of ensuring the effective and complete protection of the persons concerned. In addition, the "concept does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions."²²

52. In accordance with the Opinion 1/2010 of the Group of 29 on the concepts of "controller" and "processor", the Litigation Chamber assesses the role and status of controller *in practice*.²³
53. In this case, the defendant is responsible for storing the contact details of the website users, as the defendant has determined the means and purposes of the processing (sending invitation e-mails).²⁴ As for the means and conditions for the processing, for example, the retention period of contact details is decided by the defendant under Article 11 of its privacy policy. This period is 3 months after the account closure of the user, or immediate erasure when the website user deselects "*Contact Sync*".²⁵
54. The defendant is also in this case the controller of personal data consisting of sending invitation e-mails in the name and on behalf of "*W*" to contacts of current users.
55. However, the transfer to the recipients of the invitation e-mails and the processing of personal data in the message itself is not covered by the GDPR to the extent that the exception "household exemption" applies, i.e. in the case of a purely personal or household activity within the meaning of article 2.2 of the GDPR.
56. The defendant himself cannot invoke this exceptional "household exemption", as clarified in recital 18 of the GDPR: "This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities. ". The

²² See e.g. CJEU, C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, paras 27-29.

²³ See Working Party 29, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169), as illustrated by the Belgian DPA in a note " Overview of the concepts of controller/processor in the light of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data (GDPR) and some specific applications for professions such as lawyers; see also CPVP, Decision of 9 November 2008 regarding the control and recommendation procedure regarding SWIFT, p. 5.

²⁴ See Opinion 5/2009 of Working Party 29 on online social networking, June 12, 2009 (WP163), p. 5: "Providers of social network services are data controllers within the meaning of the Data Protection Directive. They provide the means for the processing of user data and provide all the basic services related to user management (eg, opening and deleting accounts).".

²⁵ Privacy policy dated 02-15-2019 –annex 5 to the inspection report.

defendant is responsible for sending invitation e-mails even though the user of the website can invoke the household exemption regarding the processing of personal data related to him.

57. The defendant does not contest that the GDPR applies to the processing operations at stake and does not invoke the household exception.²⁶

2.2 Clarification with regard to the household exemption and the concept of "*personal communication*".

58. The defendant states that he considers the invitation e-mails as a "*personal communication*".

In his conclusion and during the hearing, the defendant explained that this defense has nothing to do with the exception "*household exemption*" and that he never claimed that the GDPR would not apply. According to the defendant, the concept of "*personal communication*" merely refers to the fact that it is not a marketing message within the meaning of Article 13.2 of the ePrivacy Directive according to the criteria defined by Working Party 29 in the Opinion 5/2009 on online social networking.

59. The defendant therefore does not contest the application of the GDPR and that he is the controller, as regards sending out invitation e-mails.²⁷

60. In addition, the Litigation Chamber finds that if the recipients of the invitation e-mail from the online social platform are predetermined (e.g. pre-ticked), the user of the website in question has no control over an important aspect (indicating the recipients) of the purposes of the processing. The pre-ticking of recipients by the defendant is thus an additional element for the defendant to be regarded as a controller.

61. Finally, it is therefore established that the defendant is responsible for the processing of personal information of the users of the website "*W*", both in terms of storage of this data and as regards sending an invitation e-mail.

²⁶ Conclusion defendant, p. 22.

²⁷ See on this also Art 29 Working Party 29 , Opinion 5/2009 on online social networking (p.11) stating that if the recipients of an invitation e-mail are pre-determined (e.g., ticked in advance) through the online social platform, the message cannot be considered a "*personal communication*". It is then a commercial message for the benefit of the social media network in accordance with Article 13.2 of the ePrivacy Directive (Groep 29, Opinion 05/2009 on social networks, 12 June 2009 (WP 163), p. 11.).

2.3 The legal basis for processing the contact details of users and non-users of the website "W"

62. As data controller in the context of the "*Invite a friend*" feature, the defendant must ensure that this processing complies with the principles of data processing and is legitimate in the sense that the process rests on a proper legal basis (art. 5 and 6 GDPR).
63. The processing concerns personal data of users and non-users of the website "W", and is twofold: storing the contact details on the defendant's servers and sending invitation e-mails.
64. The defendant invokes that the procedure elaborated on the website "W" ensures that he obtains free, specific, informed and unambiguous consent from the user of the website, in accordance with the requirements of articles 4.11, 6.1 and 7 of the GDPR with regard to the "*Invite a friend*" feature (conclusion defendant, p. 19).
65. In particular, the defendant raises that the consent of the recipient of the message is not required, neither to store their contact details on the servers of the website, or to send an invitation e-mail, and this because the user of the website has given consent to import his address book:

"First and foremost it should be noted that the import of contact details of the contacts is a processing of personal data that is part of the purpose of the "invite a friend" feature. As explained above, Y has processed for this purpose personal data contained in the address book of a user who has given his consent. Y can therefore invoke a valid legal basis for the import of the personal data of these contacts. " (conclusion defendant, p. 21)

66. The defendant reiterated this argument during the hearing and has also made clear that he has no other legal basis he wishes to invoke.
67. The defendant also refers to other online services where users can "upload" their address book (Gmail, Hotmail, Whatsapp and Messenger) and to operating systems (such as iOS, Android and Windows) where users upload their address book and photos:

"If the Inspection Service seeks show that whenever a service user uploads personal data relating to people he knows, the company proposing this service, must obtain the consent of these people, this would undermine the operation of online communication in general. Such a position would not only apply to "invite a friend" features such as Y and other online social networking sites, but also (i) messaging services such as Gmail, Hotmail, Whatsapp and Messenger, where users upload their address book, on (ii) operating systems such as iOS,

Android and Windows, where users upload their address book and photos, and on (iii) other services such as booking services and aircraft check-in services, where users can upload personal data of people they know, etc. ".²⁸

3. Motivation and decision regarding the merits of the case

3.1 The processing of personal data of non-users

3.1.1 No valid consent

68. The Litigation Chamber does not follow the defendant in his statement that the user of the social media website may give his own consent to import third party personal data from third parties into his address book, with a view to sending an invitation e-mail.
69. Under the GDPR, only the data subject whose personal data are being processed can give valid consent to the processing of this data, except for cases of parental consent (Art. 8.1 GDPR) or any legal mandate.²⁹ In the hypothesis that data from a third party are used, this third party must give consent in accordance with the requirements laid down in Article 7 and Article 4.11 of the GDPR, as interpreted by the Group of 29.³⁰ No such consent is given here. In addition, this consent can *de facto* solely be given by existing members of "W"; if and to the extent - at the time they join the platform - they would have consented to the use of their personal data in accordance with the terms of the GDPR.
70. In this context, the Litigation Chamber also points to a study by the Dutch Data Protection Authority on Whatsapp, dating from before the entry into force of the GDPR. In the context of the mobile application Whatsapp, this authority ruled that the user of social media cannot give valid consent in the name and on behalf of a non-user of the social media platform: "*Whatsapp users cannot give (unambiguous) consent on behalf of the non-users in their address book for a processing by WhatsApp of their contact details, without being authorized by the non-users involved. Only the non-users involved (or their legal representatives) can give such consent. Since WhatsApp does not obtain unambiguous consent from non-users in the address book of Whatsapp*

²⁸ Conclusion defendant, p. 22, see also letter defendant 9 March 2020.

²⁹For an application of these principles, see for example the letter from the Working Party 29 dated October 20, 2017 to "Sinc.ME", footnote 2, available via the following webpage : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwim5d6nlr_IAhUQyKQKHWV1BCAQFjAAegQIARAC&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fjust%2Fdocument.cfm%3Fdoc_id%3D47966&usg=AOvVaw2bxnDXC8XXENQ-UdNiNDLs.

³⁰Working Party 29 Guidelines for consent under Regulation 2016/679 (WP 259 rev01), April 10, 2019.

*users for the processing of their personal data but still carries out this processing, and WhatsApp also has no basis for this data processing, WhatsApp acts in breach of Article 8 of the (Dutch) Data Protection Act.³¹*³²

3.1.2 Possibility to invoke a legitimate interest

71. In this case, no other legal basis than the "*consent*" is invoked by the defendant. The defendant invokes a "*legitimate*" interest by way of subordinate claim in its answer to the questions raised by the Litigation Chamber after the reasoned and relevant objection raised by the Netherlands. The Litigation Chamber therefore examines whether the contested processing of personal data of non-users has a legal basis under Article 6 GDPR, and whether the processing is therefore "*lawful*" or not within the meaning of Article 5.1 GDPR.
72. In the absence of any possibility to request consent regarding the processing of personal data of non-users, the Litigation Chamber examined to what extent the social media platform "*W*" could process the data of third party non-users based on its legitimate interest (art. 6.1.f) of the GDPR, with a view to precisely defined purposes, as explained below.
73. The Litigation Chamber understands that the website "*W*" has an interest to process third party non-users' personal data in order to encourage an increase in the number of members of the platform.
74. In this case, the data of third party non-users are not only processed for the purpose of identifying members of the website "*W*". The contact details (including third party non-users) are potentially kept three months by the website after the user has closed a "*W account*".³³
75. The website "*W*" also processes potentially more data than necessary to send an invitation e-mail as the concerned types of data are not defined by the website itself in a limitative way (ex. names, phone numbers and e-mail addresses): on the contrary, the processed data include potentially other types of data determined by third party providers of information society services, i.e. "*other*

³¹Article 8 of the former Data Protection Act implemented article 7 of the Data Protection Directive and equals article 6 GDPR.

³²Executive Protection of personal data, Investigation of the processing of personal data within the mobile WhatsApp application by WhatsApp Inc. dated January 15, 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf, p. 32. Decision of the CBP, the legal predecessor of the Dutch Autoriteit Persoonsgegevens.

³³ Letter from the defendant to the Inspection Service dated 14 June 2019.

information as illustrated on the permission screen of the provider, about importing your contacts on our servers".³⁴

76. Article 6.1.f of the GDPR states that the legal ground can be used in so far " *the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"
77. The case law of the Court of Justice of the European Union requires that in order to invoke Article 6.1.f) AVG a controller must fulfil "*three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence*".³⁵

78. In other words, the controller must demonstrate that:

- 1) The interests pursued by the processing, can be recognized as *legitimate* ("purpose test");
- 2) The intended processing is *necessary* for the purposes of the intended processing ("necessity test"), and
- 3) The *balancing* of these interests against the fundamental rights and freedoms of the persons concerned by the data protection weighs to the favour of the controller or of a third party ("balancing test").

➤ **Purpose test**

79. The Court of Justice clarifies that the legitimate interests "*must be present and effective as at the date of the data processing and must not be hypothetical at that date.*"³⁶
80. The Litigation Chamber also refers to the recent Guidelines 3/2019 on processing of personal data through video devices³⁷. In these guidelines the EDPB repeats that the controllers or third parties could pursue legitimate interests of a varied nature, such as legal, economic and immaterial

³⁴ Conclusion of the defendant, p 11, and a letter of the defendant to the Inspection Service dated 14 June 2019.

³⁵ CJEU, 4 May 2017, C-13/16, Rīgas, ECLI:EU:C:2017:336, para 28, ECLI:EU:C:2019:1064, and 11 December 2019, C-708/18, Asociația de Proprietari bloc M5A-ScaraA "M5A-ScaraA", para 40.

³⁶ CJEU, 11 December 2019, C-708/18, TK t/ Asociația de Proprietari bloc M5A-ScaraA, para 44.

³⁷ EDPB, "Guidelines 3/2019 on processing of personal data through video devices", 29 January 2020, nr. 18.

interests.³⁸ In this context, the EDPB also refers to the ruling of the Court of Justice that "*there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest*".³⁹

81. Based on the Court's case law and the guidance of the EDPB, the Litigation Chamber takes the view that the legal ground of legitimate interest potentially includes a wide range of interests, provided that these interests are sufficiently specific. In the context of the present case, the Litigation Chamber does not need take a position on the question whether, as such, an economic interest could qualify as a legitimate interest under Article 6.1.f, GDPR.
82. *In the present case* the defendant states that "*The objective of the W platform exists in essence in allowing users to connect with each other and to have interesting conversations and exchanges with other users*", and that
 - *Y, as controller has an interest to offer the users a possibility to find contacts that are already user and/or contacts that are not yet users and invite them to become members;*
 - *The user of W, as a third party or as a controller using the platform under the household exception (recital 18 GDPR) has an interest in finding and inviting persons he or she knows in order to easier extend his network.*"⁴⁰
83. The defendant also claims that the development of the "*invite a friend*" feature was driven by the fact that certain users asked to have an easy way to find or invite persons they know and that the experience on the social platform "W" becomes more pleasant by this "*invite a friend*" feature. The defendant underlines that this interest is a real and present interest that is neither vague nor speculative.
84. The Litigation Chamber rules that the defendant – on the basis of these facts and arguments – sufficiently shows the existence of a legitimate interest, that this interest is sufficiently specific, as follows from the detailed submissions of the controller.

³⁸ The guidelines refer to Opinion 06/2014 of the Working Party 29 on notion of "legitimate interest of the data controller" (WP217).

³⁹ Arrest Rigas, C-13/16, para 29.

⁴⁰ Letter defendant, 9 March 2020, p. 4.

➤ **The necessity test**

85. The Court of Justice clarifies that the test of necessity requires to ascertain "*that the legitimate data processing interests pursued [...] cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.*"⁴¹
86. The Court of Justice also ruled that the condition of necessity should be assessed in connection with the principle of data minimisation as laid down in article 5.1.c), GDPR.⁴²
87. The defendant claims that the "W" platform only processes elementary contact details of the contacts of its users.⁴³ It appears from the facts of the case that the defendant retains the personal data in principle for a period of three months, unless the user of the platform decides to end the synchronization of his contacts.
88. The Litigation Chamber rules that the collection of these contact details – by users and by non-users of the website – would only comply with the criterion of necessity, in so far as these details are deleted immediately after their initial use.
89. The Litigation Chamber decides in connection to non-users that it would be possible for the social media platform "W" to base itself on legitimate interest, however solely to identify existing members of the "W" platform, in order to help the users to identify their contacts that are already member of "W" and, hence, consented to use the messaging feature of the de website "W" as communication tool.
90. It is in this context relevant that these members have given their unambiguous consent to "W" in order to collect their mobile phone number or their email and to use for this purpose. In addition, "W" should implement the appropriate technical and organisational measures in order to comply with the requirements of data protection by design and by default under article 25 GDPR.
91. The Litigation Chamber refers in this context also to the Opinion 5/2009 of Working Party 29 on online social networking which states that social media networks have no other basis for processing data of non-users than the legitimate interest, and that it is not possible to invoke this basis to retrieve contact details of non-members from uploaded address books and to use them

⁴¹ TK t/ Asociatia de Proprietari bloc M5A -Scara A Rigas, para 47.

⁴² Ibid., para 48.

⁴³ Letter defendant to Litigation Chamber, 9 March 2020, p. 6.

for the creation of new social media profiles: "*Many social network services allow their members to give information about others, such as adding a name to a picture, assigning ratings to people, drawing up lists of people who want to meet or have met members. Through these tags non-members can also be identified. However, the processing of such data about non-members by a social networking service is only allowed if one of the criteria in Article 7 of the Data Protection Directive [now Article 6.1.f GDPR "legitimate interest"] is met. There is no legal basis for creating ready-made profiles of non-members by collecting data provided independently by members, including relationship data derived from uploaded address books.*"⁴⁴

92. This opinion is still relevant in principle, since the legal basis of legitimate interest has not been substantially modified since the entry into force of the GDPR. The defendant claims that he does not create profiles, but only sends invitation emails to non-members on the basis of contact details. However, this does not make the sending of those emails necessary for the purpose pursued.
93. The Working Party 29 has refined this opinion and the general interest of social media networks defined in the context of invitation e-mails, given the fundamental rights and freedoms of third party non-users. The Working Party 29 explained in its opinion regarding the notion of "*legitimate interest*", the limitations of the legitimate interest regarding third party contact details by way of example:⁴⁵

"Example 25: Access to mobile phone numbers of users and non-users of an app: 'compare and forget'

"Personal data of individuals are processed to check whether they had already granted unambiguous consent in the past (i.e., 'compare and forget' as a safeguard). An application developer is required to have the data subjects' unambiguous consent for processing their personal data: for example, the app developer wishes to access and collect the entire electronic address book of users of the app, including the mobile phone numbers of contacts that are not using the app. To be able to do this, it may first have to assess whether the holders of the mobile phone numbers in the address books of users of the app have granted their unambiguous consent (under Article 7(a)) for their data to be processed. For this limited initial processing (i.e., short-term read access to the full address book of a user of the app), the app developer may rely on Article 7(f) as a legal ground, subject to safeguards. These safeguards should include technical and organisational measures to ensure that the company only uses this access to help the user identify which of his contact persons are already users, and which therefore had already granted

⁴⁴Opinion 5/2009 of the Working Party 29 on online social networking (WP163), p. 9.

⁴⁵Opinion 6/2014 of the Working Party 29 on the notion of "legitimate interest of the data controller" (WP217).

unambiguous consent in the past to the company to collect and process phone numbers for this purpose. The mobile phone numbers of non-users may only be collected and used for the strictly limited objective of verifying whether they have granted their unambiguous consent for their data to be processed, and they should be immediately deleted thereafter".⁴⁶

94. In summary, the Working Party 29 is of the opinion that, in the circumstances described in the example above, third party contact details of non-users should only be used to check whether or not they already a member of the website, and therefore already have given their consent to use their contact details in order to communicate through the relevant website. As said, the Litigation Chamber bases its decision also on this consideration of the Working Party 29 and finds that the storage of contact details of non-users of the social media Y is only strictly necessary in the context of a "*compare and forget*" action under certain restrictive and protective safeguards.
95. The Litigation Chamber observes, however, that the retention period for these contact detail is not limited to what is strictly necessary to identify existing contacts. Moreover, the website "W" also processes potentially more data than necessary to send an invitation e-mail as the concerned types of data are not defined by the website itself in a limitative way (ex. names, phone numbers and e-mail addresses): on the contrary, the processed data include potentially other types of data determined by third party information society service providers, i.e. "*other information as illustrated on the permission screen of the provider, about importing your contacts on our servers*".⁴⁷
96. For the above mentioned reasons and circumstances, the Litigation Chamber finds that the storage of contact details of non-users of the social media Y is only strictly necessary in the context of a "*compare and forget*" action under certain restrictive and protective safeguards. These safeguards are not met.

➤ The balancing test

96. The Court of Justice clarifies that "*the assessment of that condition necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the*

⁴⁶ Zie in dezelfde zin, College bescherming persoonsgegevens, Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie WhatsApp door WhatsApp Inc. dd. 15 januari 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf, p. 32.

⁴⁷ Conclusion of the defendant, p 11, and a letter of the defendant to the Inspection Service dated 14 June 2019 - document 12 of the defendant.

particular case in question, and in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter."⁴⁸

97. The criterion relating to the seriousness of the infringement of the data subject's rights and freedoms is an essential component of the weighing or balancing exercise under article 7.1.f GDPR on a case-by-case basis.⁴⁹ In this context, the Court of Justice requires taking "*into account, inter alia, of the nature of the personal data at issue, in particular of the potentially sensitive nature of those data, and of the nature and specific methods of processing the data at issue, in particular of the number of persons having access to those data and the methods of accessing them.*"⁵⁰
98. The Court underlines that "*the data subject's reasonable expectations that his or her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data, are also relevant for the purposes of the balancing exercise.*"⁵¹. The Litigation Chamber refers in this context also to Recital 47 of the GDPR which states the importance whether "*a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.*"
99. The defendant refers in connection with the seriousness of the breach to the following specific circumstances: "*The nature of the personal data processed by Y in the context of its 'invite a friend' feature was not excessive. Y has never processed sensitive data, only the absolute minimum of personal data (i.e. elementary contact details) with one goal, namely sending of invitation emails on request and in name of the user of the W platform.*"⁵² The Litigation Chamber observes, again, that the retention period for these contact detail is not limited to what is strictly necessary to identify existing contacts. Moreover, the defendant does not define the processed contact data in a restrictive manner and also refers to any "*other information as clarified on the permission screen of the e-mail provider about importing your contacts on our servers*".⁵³.
100. The defendant refers, as concerns the reasonable expectations of the data subject, to services of online email providers such as Google, or services of providers of operating systems such as Android, IoS and Windows, or providers of social networks such as LinkedIn⁵⁴. The Litigation Chamber discusses the relevance of practices of these other providers in Section 3.1.3 below and

⁴⁸ Asociația de Proprietari bloc M5A-ScaraA "M5A-ScaraA, para 52.

⁴⁹ Ibid, para 56.

⁵⁰ Ibid, para 57.

⁵¹ Ibid., para 58.

⁵² Letter to the Litigation Chamber, 9 March 2020, p. 6.

⁵³ Conclusion of the defendant, p 11, and a letter of the defendant to the Inspection Service dated 14 June 2019.

⁵⁴ Letter to the Litigation Chamber, 9 March 2020, p. 5.

takes the view that the arguments relating to these practices fall outside the scope of the present procedure.

101. The Litigation Chamber decides in view of the above that in the present case the third condition of article 6.1, f) AVG and the case law of the Court of Justice is not fulfilled.

➤ **Conclusion**

100. The defendant could not in a legally valid manner base itself on "*legitimate interest*" as ground for the (further) processing of the personal data for direct marketing. In conclusion, the defendant infringes Article 6.1, f) GDPR.
101. Moreover, in this case, the Litigation Chamber decides that legitimate interest can only be used as legal ground for the processing of personal data of non-users with the aim of a "*compare & forget*" action, in order to select existing users amongst the contact details and to send possible invitation emails only to existing customers.
102. The Litigation Chamber decides more specifically in this case that the processing should be limited to the personal data which are strictly necessary for the purposes of "*invitation to the website*" and to the extent it is technically impossible to distinguish in the address book between members and non-members, without a minimal data processing. In addition, the defendant should in accordance with article 32 GDPR implement the appropriate technical and organizational measures to protect the processing of these data in a proper manner. Only under these conditions, the processing could be based on the legitimate interest of the defendant.
103. The Litigation Chamber takes into account that the user of the website "W" is free to send invitations through other channels (such as social media websites or e-mail providers) which are already used by the third party.

3.1.3 Defence regarding the processing of data of third persons by other information society service providers

104. The defendant compares its practices with the processing of third parties data by services such as "Whatsapp" and "Gmail", "Windows", "Linkedin".⁵⁵ The defendant states for instance that data subjects may reasonably expect that their contact details will be used by several on line service providers, because – according to the defendant it is "*common practice*" that "*an individual stores contacts details in its contact list, in order to simplify communications*".⁵⁶

105. The Litigation Chamber finds that the defence regarding the processing of personal data of third persons does not hold relevance for the reasons stated below.

106. Firstly, practices of other service providers are outside of the scope of this case.

107. Secondly, the requirement of a proper legal basis for the processing of data of non-users applies to all service providers, including those referred to by the defendant in its submissions.

108. Thirdly, these service providers may not process personal data of third parties in a manner that would affect their rights and freedoms, whatever the legal basis for the processing might be. As the Working Party 29 clearly explained in the context of the right of portability, information society service providers or telecommunications service providers should not prejudice the rights and freedoms of non-users of their services, if a user gives his consent to the storing of personal data of non-users on their servers.⁵⁷ In the context of the transfer of personal data, the Working Party 29 reiterated the inadequacy of the user consent to process data of non-users: there must be a different legal basis, and the legitimate interest of the service provider appears to be the most appropriate basis⁵⁸.

109. The Litigation Chamber considers that these views of the Working Party 29 support the earlier regarding the infringement - in this case - of the GDPR. In summary, the unlawfulness of the data processing of the website "W" is due to the fact that this website processed data of non-members without a proper legal basis, to the extent that this processing was not limited to a "*compare and forget*" action as set out above.

⁵⁵ Letter of the defendant to the Litigation Chamber, 9 March 2020, p. 5.

⁵⁶ Ibid., p. 5.

⁵⁷ Working Party 29, "Guidelines on the Right to data portability", April 5, 2017, p. 5-6: "A person who takes the initiative to send his/her data to another controller, authorizes the new controller to process the operating data or concludes a contract with that data controller. When the data set also includes personal data of a third party, another legal basis has to be found for processing. [...] For example, at a webmail a service can be created with list of contacts, friends, acquaintances, relatives and the wider environment of the individual, [...] Therefore, to avoid any breaches of third parties, the processing of such personal data by another controller is permitted only when the data remain under the exclusive control of the requesting user and managed only for purely personal or household activities. A receiving "new" data controller (to whom the data can be transmitted at the request of the user) may use the transmitted data to third parties not use for their own purposes, such as to offer those other third parties involved marketing products and services to imagine [...] Otherwise such processing in all probability is illegal and unfair, especially if the third parties were not informed of their rights as stakeholders cannot exercise their rights".

⁵⁸ Ibid.

3.1.4 Personal data of non-users used to send invitation e-mails

110. The Litigation Chamber considers that storing contact details of non-users of a website in order to send an invitation e-mail is only allowed in the context of a "*compare and forget*" action, as set out above. Therefore it is only possible to send invitation e-mails to existing members via the website "*W*". The Litigation Chamber will therefore only discuss the existence of a legal basis with regard to sending invitation e-mails to non-users in the remainder of this decision.

111. As previously mentioned, the defendant stated that the invitation e-mails are a "*personal communication*" in respect of the user of the website "*W*" so that it does not require a separate legal basis for sending this message. However, the defendant, stated in his conclusion and confirmed at the hearing that he does not intend to invoke the exception "*processing in the course of a household activity*" from Recital 18 of the GDPR.⁵⁹

112. By "*personal communication*", the defendant means that these invitation e-mails do not constitute a marketing message, except that advertising messages by e-mail - without exception - can only be sent after prior permission (see Article 13.2 of the ePrivacy Directive⁶⁰ and its implementation in Article VI.110 § 2 of the Code of Economic law).⁶¹

113. In its Opinion 5/2009 on online social networking⁶², the Working Party 29 outlines under which conditions invitation messages sent via a social media platform do not constitute an online advertising message for the platform:

"Some social networking services allow their users to send invitations to third parties. The ban on the use of e-mail for direct marketing does not apply to personal communications. The exemption for personal communication only applies if the social networking service meets the following conditions:

- there is no pressure exerted on the transmitter or receiver;*

⁵⁹See above under heading 2.1 Qualification of the data controller and of the litigious processing.

⁶⁰ "Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use."

⁶¹Article VI.110 § 2 of the Code of Economic Law provides: "Subject to Article XII.13 the use of other techniques for transmitting unsolicited communications for purposes of direct marketing referred to in paragraph 1 is permitted if the addressee, natural or legal person, here evidently not objected or, in respect of direct marketing to subscribers, provided it is in compliance with the provisions in articles VI.111 to VI.115."

⁶²Opinion 5/2009 on online social networking (WP163).

- *the provider should not choose the recipient of the message (i.e. the practice by some SNS to send invitations indiscriminately to the entire address book of a user is not allowed);*
- *the identity of the user sending the message should be clearly indicated;*
- *the user sending the message must be aware of the full content of the message to be sent on his behalf.*⁶³

114. The defendant refers to implementing these four conditions⁶⁴, and therefore believes he can send these messages without prior consent.

115. The fact that sending marketing e-mails is partly regulated by the ePrivacy Directive does not affect the competence of the Litigation Chamber to supervise the application of the GDPR with regard to the consent requirement or conditions for invoking the legitimate interest.⁶⁵

116. In this context, the Litigation Chamber decided that the social media network "*W*" should not, basically, request consent to send e-mail messages that users send to other users if the four conditions set out in the Opinion social media are met, subject to compliance with all other GDPR principles such as Article 25 (data protection by design and by default).

117. In that case, "*W*" can invoke its legitimate interest, including for storing the data on its servers, provided that the data of non-members are immediately deleted as soon as it appears that the user has not selected the recipient for the purpose of sending an invitation e-mail.⁶⁶

118. However, the Litigation Chamber considers that in respect of the strict GDPR rules with regard to the consent, also applicable in the context of the ePrivacy Directive, leave no room for such tolerance, and that the legal basis "*legitimate interest*" should be interpreted restrictively to the extent that data of third parties are involved.⁶⁷

119. Regarding the consent, Article 4, paragraph 11 with Article 7 of the GDPR defines states that the consent of the data subject means the following:

⁶³Ibid., P. 11.

⁶⁴Conclusion of the defendant, p. 23.

⁶⁵As explained by the EDPB in its advice on the Interplay between ePrivacy and GDPR: "Data Protection Authorities are competent to enforce the GDPR. The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR."

⁶⁶See explanation on the limits of the legitimate interest under Title 3.1.2.a of this decision.

⁶⁷Working Party 29 Guidelines on consent under Regulation 2016/679 (WP 259 rev01), April 10, 2019, p. 9: "With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC should be read as references to the GDPR. This includes references to approval in the current Directive 2002/58/EC [...]. Article 95 GDPR has not imposed additional obligations regarding processing associated with the provision of publicly available electronic communications services in public communications networks in the Union, provided they are subject under the e-Privacy Directive to specific obligations with the same objective. WP29 notes that the requirements for approval are not considered under the GDPR as an "additional duty", but as a precondition for lawful processing. Therefore, the requirements of the GDPR for obtaining valid consent apply in situations falling within the scope of the e-Privacy Directive."

- free;
- specific;
- informed and;
- unambiguous indication of the data subject's wishes by which he or she, accepts through a statement or a clear affirmative action, the processing of personal data.

120. In addition, this consent must be obtained prior to the processing, as is apparent from the preamble of Article 6.1 of the GDPR: *the processing is only lawful if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes, [...]]*".⁶⁸

121. Therefore, the Litigation Chamber believes that the GDPR does not allow sending e-mails to third parties with a view to obtaining their consent. This reasoning applies to the requirement of consent under the GDPR (requirement of a legal basis) and under the ePrivacy rules (requirement of "opt-in" for sending marketing messages)⁶⁹.

122. Furthermore, the Working Party 29 clearly states in its Opinion 5/2009 on online social networking regarding online social media that sending non-members of a social media website an invitation by e-mail to get access to their data is contrary to the prohibition in Article 13, paragraph 4 of the ePrivacy Directive:

*"To create ready-made profiles of non-members by collecting data which are provided independently by members, including relationship data inferred from uploaded address books, has no legal basis. Even though the social networking service would enable the non-user to inform about the existence of personal data relating to him, then a possible invitation by e-mail to join in order to gain access to the personal data is contrary to the prohibition in Article 13, paragraph 4 of the ePrivacy Directive on the sending of unsolicited electronic mail for direct marketing purposes."*⁷⁰

123. With regard to the legitimate interest, the Litigation Chamber rules that this legal basis does not allow sending such e-mails, given the impossibility for the third party to exercise control over its

⁶⁸ The Working Party 29 confirms that consent prior to the start of the processing must be achieved, Guidelines for consent under Regulation 2016/679, April 10, 2019, p. 20.

⁶⁹ Article 1(2) of the ePrivacy Directive reads as follows: "*The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.*" References to the repealed Directive 95/46/EC shall be construed as references to Regulation 2016/679 (GDPR).

⁷⁰Opinion 5/2009 on online social networking (WP 163), p. 9.

data in the context where those data were first uploaded to the website servers then used in the context of an invitation e-mail.

3.2 Storing personal data of existing users under the contacts of the person and sending invitation e-mails to existing users (contacts)

124. The defendant invokes the consent of the users for storing contact details of other users on its servers and for processing that data in the context of invitation e-mails.

125. However, the Litigation Chamber finds that the users' consent was not free to the extent that the first version of the website pre-selected the recipients of the invitation e-mails. This is the direct consequence of Recital 32 of the GDPR. The Court of Justice confirmed in *Planet49* that consent is not validly obtained if pre-ticked boxes are used:

"51. Article 2(h) of Directive 95/46 defines 'the data subject's consent' as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

*"52 Thus, as the Advocate General stated in point 60 of his Opinion, the requirement of an 'indication' of the data subject's wishes clearly points to active, rather than passive, behaviour. However, consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of a website user."*⁷¹

126. As long as the recipients of the e-mails were ticked in advance, the defendant could therefore not invoke the legal basis of "*consent*" with regard to the storing of the contact details of existing users, and sending invitation e-mails to existing users.

127. The Litigation Chamber considers that the processing in question is not necessarily unlawful within the meaning of Article 5.1 of the GDPR, and that the social media network "*W*" basically should not request an GDPR consent for sending e-mail messages from users to other users, to the extent such reports would fall under the legal basis "*necessary for the performance of a contract*" or "*legitimate interest*" (Article. 6.1.b or Article 6.1.f of the GDPR).

128. In particular, the website may invoke its legitimate interest if the e-mails do not constitute a marketing message within the meaning of Article 13.2 of the ePrivacy Directive, provided that the

⁷¹CJEU, 1 October 2019, C-673/17, *Planet49*, paras 51-52.

defendant complies with the conditions set out by the Working Party 29 (such as for example not letting the website itself determine the recipients).

129. In this case, the Litigation Chamber notes that the recipients of the invitation e-mails were originally ticked beforehand.

130. Even if the defendant does not invoke these legal bases, the Litigation Chamber observes that ticking the recipients beforehand would be problematic in the context of the legal basis of "*legitimate interest*" or "*performance of a contract*": sending e-mails in bulk does not correspond to the principle of data minimisation (Article 5.1.c GDPR) and the principles of Article 25 GDPR (data protection by design and by default). It does not matter whether the website user had the option to deselect the pre-ticket recipients one by one in the previous version of the website.

131. Finally, since the defendant voluntarily removed the pre-ticked options - in response to the grievances of the Inspection Service in this respect -, the controller "*W*" is eligible to send such e-mails based on its legitimate interest in the name and on behalf of its users to other users.

132. As an alternative to the legitimate interest, the Litigation Chamber believes that the social media network "*W*" basically had not to ask GDPR consent to send e-mail messages from users to other users, as far as such messages by "*W*" could fall under the legal basis of "*necessary for the performance of a contract*" (art. 6.1.b of the GDPR). The possibility of invoking such a basis obviously depends on the definition of the service provided and the extent to which the persons concerned have been informed about it⁷². The Litigation Chamber does not have sufficient facts to judge the lawfulness of the processing under the legal basis of "*performance of a contract*", but decides that the processing could at least be carried out under the legal basis of "*legitimate interest*", and therefore was not unlawful after removal of the pre-selection of recipients of the invitation e-mails. Finally, the Litigation Chamber observes that the defendant should be transparent about the legal bases used for processing.

3.3 The grievances of the Inspection Service with respect to the data protection officer

133. Furthermore the Litigation Chamber decides not to follow the grievances of the Inspection Service regarding the data protection officer, given the *prima facie* expertise of this person shown by the submitted resume, and the documents and the hearings show that this person duly has been involved

⁷² Zie EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

in developing the "*invite a friend*" feature. In addition, at the hearing the defendant has sufficiently explained the role and position of the data protection officer.

3.4. The defence regarding the lack of concrete recommendations from the DPA

134. The defendant complains that the DPA did not propose concrete recommendations or comments regarding the "*invite*" feature in response to the letter of 12 October 2018⁷³ in which the DPA pointed out to the defendant the requirement to obtain a valid consent under the GDPR for the "*Invite a friend*" feature (p. 3 of the conclusion). The defendant gives the same accusation against the Inspection Service (conclusion, p. 5). As the defendant rightly points out (conclusion, p. 4), the Inspection Service did not propose a recommendation regarding the invitation functionality, and she chose to ask for information.

135. The task of the Inspection Service is to gather evidence regarding indications of practices that may give rise to an infringement of the fundamental principles of data protection (Article 63 and following of the DPA ACT). The Inspection Service is not responsible for providing customized advice regarding the investigated infringements. More generally: Under Articles 5.2 and 24 of the GDPR, the controller is subject to the principle of accountability. Accountability is a core feature of the GDPR. A controller cannot denounce his accountability by a claim that he did not receive sufficient guidance from a supervisory authority. Pursuant to Article 57.1.d) of the GDPR, any supervisory authority must promote the awareness of controllers and processors as regards their obligations under the GDPR. However, the GDPR and the DPA ACT let the DPA – including its Inspection Service – a large discretion as to whether or not ask the attention of a controller for a possible infringement.

3.5 Decision regarding the sanction

136. Following the inspection report and taking into account the arguments of the defendant, the Litigation Chamber has identified the following infringements of the GDPR:

1. The defendant has no legal basis for storing the personal data of non-users of the website "W" in its files and for further processing them with a view to sending an invitation e-mail: This constitutes an infringement of Articles 5 and 6 of the GDPR;

⁷³ Answer to a letter of 3 July 2018.

2. The defendant has no legal basis for sending invitation e-mails to existing users of the website during the period in which the recipients of the invitation e-mails were ticked beforehand: infringement of Article 5.1 in conjunction with 6.1.a), 7 and 4.11 of the GDPR.

3.5.1. Jurisdiction of the Litigation Chamber with regard to sanctions

137. Pursuant to Article 100 of the DPA ACT, the Litigation Chamber has jurisdiction to order that the processing is brought into line (Art. 100.9 DPA ACT) and to impose penalties (art. 100.2° DPA ACT). The Litigation Chamber is also empowered to impose administrative fines (Art. 100.13°, 101 and 102 DPA ACT) and to publish the decision on the website of the Data Protection Authority (Art. 100.16° DPA ACT). In determining the level of the fines, the Litigation Chamber must take into account the criteria outlined in Article 83 of the GDPR depending on the circumstances. In the present case, the Litigation Chamber considers the following circumstances which it considers sufficient to sustain the decision relating to the sanction:

- the nature, severity and duration of the infringement: this is a lack of legal basis, which is a serious infringement according to the Litigation Chamber, in particular as regards the right of non-members of the website "W" to keep control over their data and not to run the risks of data processing (Recital 75 GDPR);
- the intentional nature of the infringement: the defendant was aware of a problem with regard to the processing of personal data on the website since the first letter from the DPA of 12 October 2018.

3.5.2. The mitigating circumstances invoked

138. The defendant is in subordinate order of the opinion that the sanctions pronounced should take into account the following mitigating circumstances (conclusion, p. 42):

- The defendant has not been "*negligent*" and would have acted in good faith taking into account the Opinion 5/2009 of the Working Party 29 on online social networking. The Litigation Chamber states that the defendant cannot simply rely on an opinion from 2009, long before the establishment of the GDPR, which moreover - as described above - is not sufficiently clear. In addition, the controller could have kept abreast of the discussions on the use of social media sites of data from non-members, as shown in Opinion 06/2014 of the Working Party 29 on the notion "*legitimate interest*";

- Any possible infringements would not have caused any material damage: Here, the Litigation Chamber notes that the right to data protection is a fundamental right and that the subsistence of any material damage is not relevant in order for such a right to be infringed⁷⁴. The infringements in this particular cause a loss of control over the personal data of many individuals which is explicitly referred to in paragraph 75 of the GDPR as potential non-material damage;
- The defendant stopped using pre-ticked options. The defendant was aware of the infringement since 3 April 2019 (conclusion, p. 42) and has awaited receiving a second letter from the Inspection Service (May 2019) to stop this practice (conclusion of the defendant, p. 13). The Litigation Chamber believes that this infringement was intentional or at least caused by grave negligence, since it is clearly established in Recital 32 of the GDPR that a consent is not valid if the offered options are ticked in advance.⁷⁵ The defendant therefore had to know that the consent of the users of the website to process their data in order to send invitation e-mails was not valid as regards the selection of the recipients. In addition, a controller is supposed to know that a website user is not in a position to provide consent for the use of personal data of third persons.

139. In their reaction of 28 April 2020 entered on the form, the defendant developed additional arguments with regard to the penalty proposed by the Litigation Chamber.

140. The defendant argues that they were not negligent and that the alleged infringements did not constitute a clear breach of the GDPR, but rather "*a problem of interpretation in which regard even the supervisory authorities adopt different standpoints.*" The defendant wrongly deduced this from the fact that the Dutch authority had adopted⁷⁶ a relevant and reasoned objection. The Dutch authority did not object to this final decision, and all the authorities concerned have validated the reasoning set out above regarding the amount of the fine.

141. The Litigation Chamber agrees with the defendant that a discussion was possible on the extent to which the defendant could or could not invoke a legitimate interest to address third party non-users by means of an invitation e-mail.

142. However, the Litigation Chamber found that no discussion was possible and ruled that the legal basis invoked by the defendant was invalid: the existing users of a website cannot give permission on

⁷⁴ Cour of Appeal, Brussels, 9 October 2019, "DPA v. Installé Marc" 2019/AR/1006.

⁷⁵ As clarified later in CJEU, 1 October 2019, C-673/17, Planet49, paras 51-52 (see above).

⁷⁶ As explained to the defendant in the context of the reopening of the debates on legitimate interest, the Netherlands in this case asked for more references to the case law of the Court of Justice as regards the analysis of the defendant's legitimate interest to send invitations to third parties who are not members of its social media platform, on the one hand, and disputed the relevance of references to a research report from 2013 concerning the legitimate interest of a social medium to send invitation emails, on the other hand.

behalf of third party non-users⁷⁷. The defendant thus misapplied the legal basis "*consent*" (or exemption from consent), and it is in any case not permissible to invoke the legal basis "*legitimate interest*" a posteriori in order to justify⁷⁸ processing which has already started.

143. For the sake of clarity, the Litigation Chamber reminds the defendant that it did not invoke the "*legitimate interest*" basis (and did not examine its conditions of application) in its original privacy policy, nor later in the context of its arguments before the Litigation Chamber, despite a clear question from the Litigation Chamber in that respect at the hearing, and up to and including the reopening of the debates by the Litigation Chamber on that point. This constitutes a clear breach of their information obligations set out in Article 12-13 GDPR and the requirement under Article 5-6 GDPR to have an appropriate legal basis before data processing begins.

144. It is also beyond dispute that with regard to invitations sent to existing members of the social media platform "*W*", the defendant could not invoke the legal basis of "*consent*" whereby the addressees of the invitation e-mails were originally ticked in advance⁷⁹.

145. For this reason, the Litigation Chamber decides that the defendant has been negligent and deserves a fine as regards the sending of invitation emails both to members and to third party non-members of the social media platform "*W*", and that a fine is justified, even if there was a possible debate regarding the limits and conditions of the defendant's justified interest as regards the sending of invitation emails by social media to third party non-members. In view of the circumstances presented to it, the Litigation Chamber decides upon this question in this case.

146. In determining the amount of the fine, the Litigation Chamber shall take into account the circumstances invoked under 3.5.1 and 3.5.2 of this decision.

147. The Litigation Chamber also takes note of the fact that the defendant, according to the information provided in their response of 28 April 2020, stopped the sending of invitation emails as of 07 February 2020.

⁷⁷ See reasoning under heading 3.3.1.

⁷⁸ See Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018, p. 27: "It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals. In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. **Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.**" [bolding of the Litigation Chamber]

⁷⁹ See reasoning under heading 3.2.

148. However, the Litigation Chamber did not require such a far-reaching measure and reopened the debates on legitimate interest in order to allow the defendant to properly carry out their assessment of the latter.
149. In the original draft decision, as submitted to the data protection authorities concerned in the context of the cooperation procedure provided for in Article 60.5 of the GDPR, the Litigation Chamber had ordered that the processing be brought into compliance with Articles 5 and 6 of the GDPR within 3 months of the date of this decision, by ensuring that the storage and processing of personal data for the purpose of sending invitation e-mails to third party non-members of the website be either discontinued or be founded on a legal basis (e.g. consent, legitimate interest). However, this intended order no longer has any *raison d'être* in view of the fact that the defendant - according to the statements made by their counsel in their response of 28 April 2020 - spontaneously stopped the sending of invitation emails as of 07 February 2020.
150. The fact that the defendant stopped sending invitation e-mails is a sign of goodwill, but does not alter the fact that the defendant was negligent in determining a legal basis, not only for the beginning of the data processing in question but also in the context of their reasoning submitted to the Litigation Chamber, despite the reopening of the debates by the latter. The fact that the defendant has stopped using pre-ticked options only has a positive impact on the legal basis of "*consent*" for the invitation e-mails sent to existing users, but not with regard to the third-party non-users of the website.
151. Nevertheless, it appears from the above there is a willingness by the defendant to devote attention to the GDPR in the development of the processing. This is important for determining the level of the sanction.
152. The Data Protection Authority considers that the annual turnover of the defendant from 2017 onwards (including for the financial year 2019, for which closure is still ongoing) will still exceed €10,000,000. The Litigation Chamber decided that when determining the amount of the fine that an amount of 0.5% of the annual turnover would be appropriate, and therefore set the amount of the fine at €50,000.
153. Given the importance of transparency in relation to the decision of the Litigation Chamber, this decision will be published on the website of the Data Protection Authority. Publication of the present decision is also in the interests of the development of the law and the consistent application of the GDPR in the European Union. However, it is not necessary for the defendant's identification data to be disclosed directly for that purpose.

FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation,

to impose a fine of 50,000 Euro for processing personal data of non-members of the website "W" without an appropriate legal basis, as well as personal data of members, the latter during the period in which the recipients to such e-mails were ticked in advance.

Against this decision and based on art. 108, §1 of the Act of 3 December 2017, an appeal can be lodged within thirty days after service of the notice at the Marktenhof (Court of Appeal in Brussels) with the DPA as a defendant.

[REDACTED]
[REDACTED]



Litigation Chamber

Decision XX/2021 of 17 January 2022

File number: DOS-2021-07137

Subject matter: Exercising of the right to erasure without adequate follow-up by the data controller

The Litigation Chamber of the Data Protection Authority, composed of [REDACTED]

Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the GDPR;

Pursuant to the Act of 3 December 2017 establishing the Data Protection Authority, hereinafter referred to as DPAA;

Having regard to the Internal Rules of Procedure, as approved by the Chamber of Representatives on 20 December 2018 and published in the Belgian Official Gazette on 15 January 2019;

Pursuant to the documents in the file

has taken the following decision regarding:

The complainant:

[REDACTED] residing at [REDACTED]
[REDACTED] hereinafter 'the complainant';

The data controller:

[REDACTED] with its registered office at [REDACTED]
[REDACTED] hereinafter referred to as "the data controller"

I. Facts and procedure

1. On 21 October 2021, the complainant filed a complaint with the Slovak supervisory authority against the data controller. This is a cross-border complaint within the meaning of Article 60 of the GDPR, which was referred by the Slovak supervisory authority to the Belgian Data Protection Authority. On 23 November, the [Belgian] Data Protection Authority confirmed that it would act as Lead Supervisory Authority (LSA) in this case as the data controller is the representative of a company located within the EU whose registered office is in Belgium. The supervisory authorities of the following EU Member States confirmed that they would act as Concerned Supervisory Authorities (CSA): Ireland, Sweden, Estonia and Italy. As the complaint was filed with the Slovak authority, the latter is also a CSA.
2. The complaint concerns the failure of the data controller to comply with the complainant's request to exercise her right to erasure. On 4 September, and again on the 19 September 2021, the complainant contacted the data controller requesting that the personal data relating to her be deleted. On 21 September 2021, the data controller confirmed that the complainant's account had been deleted. However, the complainant found that her name and first name still appeared on the website.
3. This complaint is the subject of the procedure provided for in Article 60 GDPR (Cooperation between the Lead Supervisory Authority and the other Concerned Supervisory Authorities). This procedure provides that the Litigation Chamber as LSA submits a draft decision to the CSAs for their consideration within a period of 4 weeks. The CSAs may submit relevant and substantiated objections which the Litigation Chamber should take into account. If no objection has been lodged within the prescribed period, the LSA and the CSAs are deemed to agree to the draft decision and shall be bound by it.

II. Reasoning

4. Based on the documents supporting the complaint, the Litigation Chamber finds that the complainant exercised her right to data erasure pursuant to Article 17.1 GDPR¹, and that the data controller subsequently confirmed the deletion of her account, as required by Article 12(3) and (4)

¹ 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

GDPR². However, the complainant found that her request for erasure was not fully complied with, as her name was still listed on the data controller's website. By doing so, the controller acted in violation of Article 17.1 of the GDPR.

5. The Litigation Chamber is of the opinion that, on the basis of the above analysis, it must be concluded that the data controller committed an infringement of the provisions of the GDPR, which justifies the adoption of a decision in this case on the basis of Article 95, § 1, 5° DPAA, i.e. ordering the data controller to comply with the complainant's exercise of their right to erasure (Article 17.1 GDPR), particularly in view of the documents provided by the complainant, which show that the data controller did not adequately comply with the complainant's request to erase the data, given that the complainant's surname and first name still appeared on the data controller's website.
6. The present decision is a *prima facie* decision taken by the Litigation Chamber in accordance with Article 95 DPAA on the basis of the complaint lodged by the complainant, within the framework of the "procedure preceding the decision on the merits"³ and not a decision on the merits of the Litigation Chamber within the meaning of Article 100 DPAA. The Litigation Chamber has thus decided to rule on the basis of art. 58.2. c) GDPR and Art. 95, §1, 5° of the Act of 3 December 2017, and thus order the data controller to comply with the data subject's requests to exercise their rights, in particular the right to data erasure ("right to be forgotten") (Art. 17 GDPR).
7. The purpose of this decision is to inform the data controller that it has breached the provisions of the GDPR and to give it the opportunity to comply with the aforementioned provisions.
8. However, if the controller does not agree with the contents of the present *prima facie* decision and considers that it has factual and/or legal arguments which could lead to a different decision, it may send an e-mail to litigationchamber@apd-gba.be to submit a request to the Litigation Chamber to examine the merits of the case within 14 days of service of this decision. If necessary, the enforcement of this decision shall be suspended for the aforementioned period.
9. In the event of a continuation of the proceedings on the merits, the Litigation Chamber shall invite the parties, pursuant to Articles 98, 2° and 3° in conjunction with Article 99 of the DAPA, to submit their defences and to attach any documents they deem useful to the file. This decision shall be permanently suspended if necessary.

² 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

³ Section 3, Subsection 2 DPAA (Articles 94 to 97).

10. For the sake of completeness, the Litigation Chamber points out that a hearing on the merits of the case may lead to the imposition of the measures mentioned in Article 100 DAPA⁴.

11. Finally, the Litigation Chamber points out the following:

If either party wishes to make use of the possibility to consult and copy the file (art. 95, §2, 3° DPAA), they should apply to the secretariat of the Litigation Chamber, preferably via litigationchamber@apd-gba.bein order to schedule an appointment. If a copy of the file is requested, the documents shall be delivered electronically if possible or otherwise by ordinary mail⁵.

III. Publication of the decision

12. Given the importance of transparency in relation to the decision of the Litigation Chamber, this decision will be published on the website of the Data Protection Authority. However, it is not necessary for the defendant's identification data to be disclosed directly for that purpose.

⁴ 1° to close a complaint; 2° to order the dismissal of a complaint; 3° to order the suspension of the judgment; 4° to propose a settlement; 5° to issue warnings and reprimands; 6° to order compliance with the requests of the data subject to exercise their rights; 7° to order the notification of the security problem to the data subject; 8° to order the temporary or definitive freezing, restriction or prohibition of the processing; 9° to order the bringing into compliance of the processing; 10° to order the rectification, restriction or erasure of data and the notification thereof to the recipients of the data; 11° to order the withdrawal of the accreditation of certification bodies; 12° to impose periodic penalty payments 13° to impose administrative fines; 14° to order the suspension of cross-border data flows to another State or international institution; 15° to transfer the file to the public prosecutor's office in Brussels, which will inform it of the action taken; 16° to decide, on a case-by-case basis, to publish its decisions on the website of the Data Protection Authority.

⁵ Due to the exceptional circumstances which have arisen due to COVID-19, the option of collection from the secretariat of the Litigation Chamber is NOT available. Moreover, all communication is in principle electronic.

ON THESE GROUNDS,

the Litigation Chamber of the Data Protection Authority rules, subject to the lodging of a request by the data controller, on the merits in accordance with Article 98 et seq. DPAA, to:

- pursuant to **Article 58.2(c) of the GDPR** and **Article 95(1)(5) of the DPAA**, to order the data controller to comply with the data subject's request to exercise their rights, in particular the right to erasure (Article 17.1 of the GDPR), and to proceed with the erasure of the personal data concerned within a period of 14 days from the service of this decision;
- order the data controller to inform the Data Protection Authority (Litigation Chamber) of the result of this decision by e-mail within the same period of time, at the e-mail address litigationchamber@apd-gba.beand
- in the absence of timely implementation of the above by the controller, to rule on the merits of the case ex officio in accordance with **Articles 98 et seq. DPAA**.

This decision may be challenged pursuant to art. 108, §1 DPAA; an appeal may be lodged with the Market Court within a period of thirty days from the service, with the Data Protection Authority as defendant.

(signature)

Hielke Hijmans

President of the Litigation Chamber



Litigation Chamber

Decision **XX/2021** of 17 January 2022

File number: DOS-2021-06120

Subject matter: Complaint regarding lack of response to request for access

The Litigation Chamber of the Data Protection Authority, composed [REDACTED]

Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the GDPR;

Pursuant to the Act of 3 December 2017 establishing the Data Protection Authority, hereinafter referred to as DPAA;

Pursuant to the Internal Rules of Procedure, as approved by the Chamber of Representatives on 20 December 2018 and published in the *Belgian Official Gazette* on 15 January 2019;

Pursuant to the documents in the file

has taken the following decision regarding:

The complainant: [REDACTED] residing at [REDACTED] hereinafter "the complainant";

The data controller: [REDACTED] with its registered office at [REDACTED], [REDACTED] hereinafter "the data controller"

I. Facts and procedure

1. On 4 July 2020, the complainant filed a complaint against the data controller with the Irish Data Protection Commission. This is a cross-border complaint within the meaning of Article 60 of the GDPR, which was referred from the Irish supervisory authority to the Belgian Data Protection Authority. On 23 November, the [Belgian] Data Protection Authority (DPA) confirmed that it would act as Lead Supervisory Authority (hereinafter LSA) in this case, as the data controller's registered office is in Belgium. The supervisory authorities of the following EU Member States confirmed that they would act as Concerned Supervisory Authorities (CSA): Sweden, Estonia, Poland, Norway and the Netherlands. As the complaint was lodged with the Irish authority, the latter is also a CSA.
2. The complaint concerns the failure of the data controller to comply with the complainant's request to exercise his rights of access and information. On 13 July 2020, the complainant addressed his request to the controller by e-mail. The complainant also sent a request for access on 14, 15, 16, 20 and 21 July 2020 via the website of the data controller. The complainant sent the controller a reminder e-mail on 31 August 2020. The complainant did not receive an answer from the controller to any of these requests.
3. This complaint is the subject of the procedure provided for in Article 60 GDPR (Cooperation between the Lead Supervisory Authority and the other Concerned Supervisory Authorities). This procedure provides that the Litigation Chamber as LSA submits a draft decision to the CSAs for their consideration. The CSAs may submit relevant and substantiated objections, which the Litigation Chamber should take into account within a period of 4 weeks. If no objection has been lodged within the prescribed period, the LSA and the CSAs are deemed to agree to the draft decision and shall be bound by it.

II. Reasoning

4. It is apparent from the documents in the file that the complainant, in accordance with Article 15 of the GDPR¹, addressed a request to the data controller to access his personal data. Pursuant to

¹ Article 15 GDPR: 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;
 (b) the categories of personal data concerned;
 (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 (f) the right to lodge a complaint with a supervisory authority;
 (g) where the personal data are not collected from the data subject, any available information as to their source;
 (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
 2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
 3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
 4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

Article 12.3 of the GDPR², the data controller was obliged to inform the complainant without delay, and in any event within one month of receipt of the request, of the action taken concerning the request. That period may be extended by a further two months if necessary, depending on the complexity of the requests and the number of requests. The data controller did not respond despite several requests from the complainant to the controller to comply with his request to exercise his rights of access and information. It is clear from the facts that the deadline for responding to the complainant's request was exceeded in every respect.

5. The Litigation Chamber is of the opinion that, on the basis of the above analysis, it must be concluded that the data controller committed an infringement of the provisions of the GDPR, which justifies the adoption of a decision in this case on the basis of Article 95, § 1, 5° DPAA; more specifically, to order the data controller to comply with the complainant's exercise of his right to access the data (Article 15 GDPR), particularly in view of the documents submitted by the complainant which show that the data controller did not respond to the complainant's request in this sense.
6. The present decision is a *prima facie* decision taken by the Litigation Chamber in accordance with Article 95 DPAA on the basis of the complaint lodged by the complainant, within the framework of the "procedure preceding the decision on the merits"³ and not a decision on the merits of the Litigation Chamber within the meaning of Article 100 DPAA. The Litigation Chamber has thus decided to rule on the basis of art. 58.2. c) GDPR and Art. 95, §1, 5° of the Act of 3 December 2017, and thus order the data controller to comply with the data subject's requests to exercise his rights, in particular the right of access (Art. 15 GDPR).
7. The purpose of this decision is to inform the data controller that it has breached the provisions of the GDPR and to give it the opportunity to comply with the aforementioned provisions.
8. However, if the data controller does not agree with the contents of the present *prima facie* decision and considers that it has factual and/or legal arguments which could lead to a different decision, they may send an e-mail to litigationchamber@apd-gba.be to submit a request to the Litigation Chamber to examine the merits of the case within 14 days of service of this decision. If necessary, the enforcement of this decision shall be suspended for the aforementioned period.
9. In the event of a continuation of the proceedings on the merits, pursuant to Articles 98, 2° and 3° in conjunction with Article 99 of the DPAA, the Litigation Chamber shall invite the parties to submit their defences and to attach any documents they deem useful to the file. This decision shall be permanently suspended if necessary.

² Article 12.3 GDPR: The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.'

³ Section 3, Subsection 2 DPAA (Articles 94 to 97).

10. For the sake of completeness, the Litigation Chamber points out that a hearing on the merits of the case may lead to the imposition of the measures mentioned in Article 100 DPAA⁴.

11. Finally, the Litigation Chamber points out the following:

If either party wishes to make use of the possibility to consult and copy the file (art. 95, §2, 3° DPAA), they should apply to the secretariat of the Litigation Chamber, preferably via litigationchamber@apd-gba.be, in order to schedule an appointment. If a copy of the file is requested, the documents shall be delivered electronically if possible or otherwise by ordinary mail⁵.

III. Publication of the decision

12. Given the importance of transparency in relation to the decision of the Litigation Chamber, this decision will be published on the website of the Data Protection Authority. However, it is not necessary for the defendant's identification data to be disclosed directly for that purpose.

⁴

1° to close a complaint; 2° to order the dismissal of a complaint; 3° to order the suspension of the judgment; 4° to propose a settlement; 5° to issue warnings and reprimands; 6° to order compliance with the requests of the data subject to exercise their rights; 7° to order the notification of the security problem to the data subject; 8° to order the temporary or definitive freezing, restriction or prohibition of the processing; 9° to order the bringing into compliance of the processing; 10° to order the rectification, restriction or erasure of data and the notification thereof to the recipients of the data; 11° to order the withdrawal of the accreditation of certification bodies; 12° to impose periodic penalty payments 13° to impose administrative fines; 14° to order the suspension of cross-border data flows to another State or international institution; 15° to transfer the file to the public prosecutor's office in Brussels, which will inform it of the action taken; 16° to decide, on a case-by-case basis, to publish its decisions on the website of the Data Protection Authority.

⁵ Due to the exceptional circumstances arising due to COVID-19, the option of collection from the secretariat of the Litigation Chamber is NOT available. Moreover, all communication is in principle electronic.

ON THESE GROUNDS,

the Litigation Chamber of the Data Protection Authority rules, subject to the lodging of a request by the data controller, on the merits in accordance with Article 98 et seq. DPAA, to:

- pursuant to **Article 58.2(c) of the GDPR** and **Article 95(1)(5) of the DPAA**, to order the data controller to comply with the data subject's request to exercise their rights, in particular the right of access (Article 15 of the GDPR), and to proceed to the transmission of the requested information within a period of 14 days from the service of this decision;
- order the Data Controller to inform the Data Protection Authority (Litigation Chamber) of the result of this decision by e-mail within the same period of time, at the e-mail address litigationchamber@apd-gba.be and
- in the absence of timely implementation of the above by the data controller, to rule on the merits of the case ex officio in accordance with **Articles 98 et seq. DPAA**.

This decision may be challenged pursuant to art. 108, §1 DPAA; an appeal may be lodged with the Market Court within a period of thirty days from the service, with the Data Protection Authority as defendant.

Hielke Hijmans
President of the Litigation Chamber



Decision on the merits 21/2022 of 2 February 2022

Unofficial translation from Dutch

Case number: DOS-2019-01377

Concerning: Complaint relating to Transparency & Consent Framework

The Litigation Chamber of the Data Protection Authority, composed of Mr Hielke Hijmans, chairman, and Mr Yves Poulet and Mr Frank De Smet;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the GDPR;

Having regard to the Act of 3 December 2017 establishing the Data Protection Authority, hereinafter referred to as DPA Act;

Having regard to the Internal Rules of Procedure, as approved by the House of Representatives on 20 December 2018 and published in the *Official Gazette* on 15 January 2019;

Having regard to the documents in the file;

has taken the following decision on:

The complainants: Mr Johnny Ryan; Mr Pierre Dewitte and Mr Jeff Ausloos, as well as Mrs Katarzyna Szymielewicz, who designated the NGO Panoptikon Foundation to act on her behalf, and the NGOs Bits of Freedom and La Ligue des Droits de l'Homme, all represented by Mr Frederic Debusseré and Mr Ruben Roex, and Mr Bruno Bidon, hereinafter 'the complainants';

The defendant: IAB Europe, having its registered office at [...] 1040 Brussels, with company number [...], represented by Mr Frank Judo and Mr Kristof Van Quathem, hereinafter 'the defendant'.

Table of contents

Case number: DOS-2019-01377	1
A. Facts and procedure.....	4
A.1. - Complaints against Interactive Advertising Bureau Europe	4
A.2. - The language of the procedure: Interim Decision 01/2021 as amended by the Interim Decision 26/2021 of 23 February 2021	6
A.3. - RTB and TCF	6
A.3.1. - Definitions and operation of the Real-Time Bidding system.....	6
A.3.2. - IAB Europe's Transparency & Consent Framework.....	12
A.4. - Reports of the Inspection Service	15
A.4.1 - IAB Europe acts as data controller in respect of the Transparency and Consent Framework and the personal data processing operations relating thereto	15
A.4.2. - Identified infringements of the GDPR	15
A.4.3. - Additional considerations that the Inspection Service considers relevant to the assessment of the gravity of the facts	19
A.5. - Summary of the defendant's response dd. 11 February 2021	19
A.5.1. - IAB Europe is not a data controller with regard to the processing of personal data in connection with the TCF	19
A.5.2. - The TCF complies with the GDPR.....	22
A.5.3. - IAB Europe is not subject to the obligation to keep a register of processing operations.....	23
A.5.4. - IAB Europe is not required to appoint a data protection officer	24
A.5.5. - IAB Europe did cooperate with the Inspection Service	24
A.5.6. - There are no aggravating circumstances to the detriment of IAB Europe	24
A.6. - Summary of the complainants' reply submissions dd. 18 February 2021	25
A.6.1. – IAB Europe is data controller for the TCF	25
A.6.2. - The processing operations carried out in the TCF violate the GDPR at various levels	26
A.7. - Summary of the defendant's rejoinder dd. 25 March 2021.....	34
A.7.1. - Organisations that process personal data within the RTB system are responsible for complying with the GDPR and the ePrivacy Directive	34
A.7.2. - IAB Europe cannot be held responsible for the alleged illegal practices of RTB participants, as the TCF is completely separate from RTB	35
A.8. - Hearing and reopening of debates	36
A.9. - Procedural objections raised by the defendant	41

A.9.1. - Infringements of procedural rules applicable to the inspection report and of fundamental rights and freedoms of IAB Europe	41
A.9.2. - Infringements of the fundamental rights and freedoms of IAB Europe with regard to the general nature of the procedure for the DPA.....	47
A.10. - Sanction form, European cooperation procedure and publication of the decision.....	58
B. Reasoning.....	62
 B.1. – Processing of personal data in the context of the Transparency and Consent Framework	62
 B.1.1. – Presence of personal data within the TCF	62
 B.1.2. - Processing of personal data within the TCF	67
 B.2. - Responsibility of IAB Europe for the processing operations within the Transparency and Consent Framework	68
 B.2.1. - Broad interpretation of the concept of data controller by the Court of Justice and the EDPB	69
 B.2.2. - Determining the purposes of the processing of personal data within the TCF	71
 B.2.3. - Determining the means for processing personal data within a TCF	74
 B.3. - Joint controllership of publishers, CMPs and adtech vendors with regard to the means and purposes of the processing of personal data within the context of the TCF and of the OpenRTB	79
 B.3.1. - Joint processing responsibility.....	80
 B.4. On the alleged breaches of the General Data Protection Regulation	87
 B.4.1 - Lawfulness and fairness of processing (Art. 5.1.a and 6 GDPR).....	87
 B.4.2. - Duty of transparency towards data subjects (Art. 12, 13 and 14 GDPR)	99
 B.4.3. - Accountability (art. 24 GDPR), data protection by design and by default (Art. 25 GDPR), integrity and confidentiality (Art. 5.1.f GDPR), as well as security of processing (Art. 32 GDPR).....	101
 B.4.4. - Additional alleged breaches of the GDPR.....	105
C. Sanctions.....	111
 C.1. - Breaches.....	115
 C.2. - Sanctions	118

A. Facts and procedure

A.1. - Complaints against Interactive Advertising Bureau Europe

1. In the course of 2019, a series of complaints were filed against Interactive Advertising Bureau Europe (hereinafter IAB Europe), for breaching various provisions of the GDPR in relation to large-scale processing of personal data. The complaints related, in particular, to the principles of legality, appropriateness, transparency, purpose limitation, storage restriction and security, as well as to accountability.
2. Nine identical or very similar complaints were filed, four directly with the Data Protection Authority (hereinafter 'DPA') and five via the IMI system with supervisory authorities in other EU countries.
3. The Inspection Service also carried out investigations on its own initiative, pursuant to Article 63(6) DPA Act. Since the complaints related to the same subject matter and were directed against the same party (IAB Europe), on the basis of the principles of proportionality and necessity in the conduct of investigations (Article 64 DPA Act), the Inspection Service merged the above files into one case under file number DOS-2019-01377.
4. The complainants have agreed to this merger, as well as to the request by the Litigation Chamber to merge their submission and submit them as a joint package, in the interests of economy and efficient proceedings.
5. In this international case, four complainants, including the NGO Ligue des Droits Humains, are domiciled in Belgium, one in Ireland, four in different EU states, represented by the Polish-based NGO Panoptikon, and one complainant is represented by the Dutch-based NGO Bits of Freedom.
6. Pursuant to Article 4(1) DPA Act, the Data Protection Authority is responsible for monitoring the data protection principles contained in the GDPR and in other laws containing provisions on the protection of the processing of personal data.
7. Pursuant to Article 32 DPA Act, the Litigation Chamber is the administrative dispute resolution body of the DPA¹.
8. Pursuant to Articles 51 et seq. GDPR and Article 4(1) of the DPA Act, it is the task of the Litigation Chamber, as the administrative dispute resolution body of the DPA, to exercise effective control over the application of the GDPR and to protect the fundamental rights

¹ The administrative nature of the disputes before the Litigation Chamber has been confirmed by the Market Court. See in particular the judgment of 12 June 2019, published on the website of the DPA, as well as decision 17/2020 of the Litigation Chamber.

and freedoms of natural persons with regard to the processing of their personal data and to facilitate the free flow of personal data within the European Union. These tasks are further explained in the Strategic Plan and the management plans of the DPA, drawn up pursuant to Article 17(2) DPA Act.

9. Moreover, as regards the one-stop-shop mechanism, Article 56 GDPR states: "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.*"
10. Article 4.23 GDPR clarifies the notion of cross-border processing in the following terms: "*processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State;*"
11. The defendant has its only registered office in Belgium, but its activities have a significant impact on stakeholders in several Member States, including the plaintiffs in Ireland, Poland and the Netherlands, as well as in Belgium. The Litigation Chamber draws its jurisdiction from a combined reading of Articles 56 and 4(23)(b) of the GDPR. The DPA was seized by the Polish, Dutch and Irish data protection authorities following a complaint made to them by the complainants in accordance with Article 77.1 of the GDPR. It declares that it is the lead supervisory authority (Article 60 of the GDPR).
12. The following supervisors have indicated their willingness to act as concerned supervisory authorities (CSA): the Netherlands, Latvia, Italy, Sweden, Slovenia, Norway, Hungary, Poland, Portugal, Denmark, France, Finland, Greece, Spain, Luxemburg, Czech Republic, Austria, Croatia, Cyprus, and Germany (Berlin, Rhineland-Palatinate, North Rhine-Westphalia, Saarland, Lower Saxony, Brandenburg, Mecklenburg-Western Pomerania, Bavaria).
13. In the course of the proceedings, additional complaints with a very similar focus to the ones on which the present case is based were sent to the Belgian DPA, by the Maltese, Romanian, Croatian, Greek, Portuguese, Swedish, Cypriot and Italian DPAs. These complaints are not part of the present proceedings.

A.2. - The language of the procedure: Interim Decision 01/2021 as amended by the Interim Decision 26/2021 of 23 February 2021

14. On 13 October 2020, the Litigation Chamber sent a letter to the parties, in accordance with Article 98 DPA Act, informing the parties of the language of the procedure (French), and inviting them to present their written submissions.
15. In response to a request by the complainants dd. 27 November 2020, and in view of the international nature of this case, the Litigation Chamber issued Interim Decision 01/2021 on 8 January 2021 regarding the language of the proceedings. Following an appeal by the complainants to the Market Court, this Interim Decision was amended on 23 February 2021 (Interim Decision 26/2021).
16. Pursuant to the latter Interim Decision, which is based on an agreement with the parties, the DPA's correspondence with the parties is conducted in Dutch and the preliminary and final decisions of the Litigation Chamber are in Dutch. However, the Litigation Chamber shall provide the parties with a French and an English translation of the final decision.
17. Moreover, the parties are free to use the language of their choice (Dutch, French or English) in the proceedings before the Litigation Chamber, either in writing or orally. In the case of IAB Europe, it is French or English. The DPA is not responsible for translations of procedural documents submitted by one party on behalf of the other.
18. Finally, the Litigation Chamber points out that it sometimes uses English language terminology in this decision, in cases where translation into Dutch would reduce the comprehensibility of the decision.

A.3. - RTB and TCF

19. In essence, this case concerns, on the one hand, the conformity of the Transparency & Consent Framework (hereinafter, 'TCF') with the GDPR and, more specifically, the responsibility of IAB Europe, the defendant in these proceedings, and other various actors involved. In addition, it also pertains to the impact of the TCF on the so-called Real-Time Bidding (RTB). Given the complexity of the latter, it is introduced here.

A.3.1. - Definitions and operation of the Real-Time Bidding system

20. In contrast to "traditional" advertising, where the parties involved manually and contractually determine the modalities of information exchange, online advertising is

usually done primarily automatically and behind the scenes, through "*Programmatic advertising*" methods of which real-time bidding (RTB) is the leading system².

21. Real-time bidding is defined in legal literature as "a network of partners that enables big data applications within the organisational field of marketing to improve sales of pre-determined advertising space through real-time data-driven marketing and personalised (behavioural) advertising"³.
22. Real-time bidding refers to the use of an instantaneous automated online auction for the sale and purchase of online advertising space. Specifically, it means that when an individual accesses a website or application that contains an advertising space, behind the scenes through an automated online *auction* system and algorithms, technology companies representing thousands of advertisers can instantly (in *real time*) *bid* for that advertising space to display targeted advertising specifically tailored to that individual's profile.
23. Real-time bidding works behind the scenes on most commercial websites and mobile apps. Thousands of companies are involved that receive information about the person visiting the website. In this way, billions of advertisements are auctioned every day.
24. In a real-time bidding system, several parties are involved⁴:
 - A. The companies or organisations that have created and manage the relevant real-time bidding system, including by setting its *policies/governance* and technical protocols. The main ones are:
 - a. the "*OpenRTB*" system and the associated "*Advertising Common Object Model*" (AdCOM), created by IAB Technology Laboratory, Inc. (abbreviated as "IAB Tech Lab") and Interactive Advertising Bureau, Inc. (abbreviated as "IAB"), both based in New York;
 - b. the "*Authorised Buyers*" system created by Google.

The OpenRTB is a standard protocol that aims to simplify the interconnection between ad space providers, publishers (ad exchanges, *Sell-Side Platforms*, or networks working with publishers), and competing buyers of ad space (bidders, *Demand-Side Platforms*, or

² M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", German Law Journal, 31 July 2021, p. 8-10.

R. VAN EJK, "Web Privacy Measurement in Real-Time Bidding Systems - A Graph-Based Approach to RTB system classification", 2019, p.140: "a network of partners enabling big data applications within the organizational field of marketing to improve sales by real-time data-driven marketing and personalized (behavioural) advertising", available at <https://ssrn.com/abstract=3319284>; ³ M. VEALE, FR. ZUIDERVEEN BORGESIUS, *ibidem*, p. 3.

⁴ *Ibidem*.

networks working with advertisers). The overall objective of OpenRTB is to establish a common language for communication between buyers and vendors of advertising space⁵.

B. On the "supply side" there are:

- a. Companies that own a website or app with advertising space. In RTB jargon, these companies are called "*publishers*".
- b. Companies operating an automated online platform through which *publishers* can optimise the value and volume of their ad space sales by signalling the availability of their ad space to be displayed to a data subject and requesting that one or more *bid requests* be made for that ad space. In RTB jargon, these companies are called "*Sell-Side Platforms*" ("SSPs"). SSPs provide the available inventory of their publishers to the various ad exchanges in the market and possibly to ad networks and other DSPs. The most advanced SSPs work in real time. As soon as an ad space is called up when a page is viewed on a publisher's site, the SSP searches for the best offer on that type of ad space according to the detected visitor profile, and automatically delivers the corresponding ad⁶.

C. On the "demand side" there are:

- a. Companies that want to display advertising for their products or services in a targeted manner to visitors to websites and users of apps (the advertisers).
- b. Companies operating an online platform that enables advertisers and media agencies to carry out and optimise their purchases of advertising space, and in which advertisers' ads are offered⁷. In RTB jargon, these companies are called "*Demand-Side Platforms*" ("DSPs").

D. Acting as intermediaries between them are companies, so-called "*Ad Exchanges*", which bring the supply and demand side organisations together and allow them to communicate with each other automatically so that the DSPs can bid on *bid requests* from SSPs.

E. In addition, there are so-called "*Data Management Platforms*" ("DMPs") that extract huge amounts and types of personal data from multiple sources (such as from devices, cookies, mobile identifiers, pixels, online surfing behaviour analysis, social media, offline data, but also from third parties such as data brokers, etc.), then centralise this data, and finally analyse and categorise it by means of algorithms and artificial intelligence. By

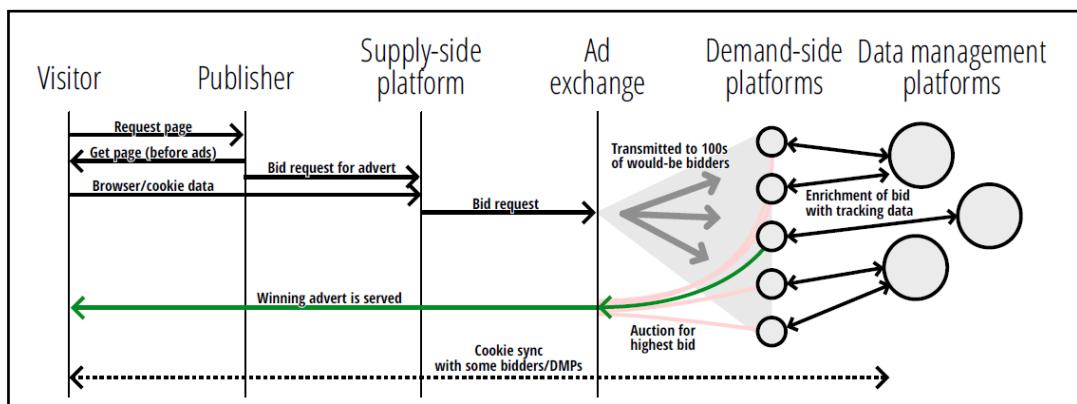
⁵ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 11.

⁶ Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), p. 5-6.

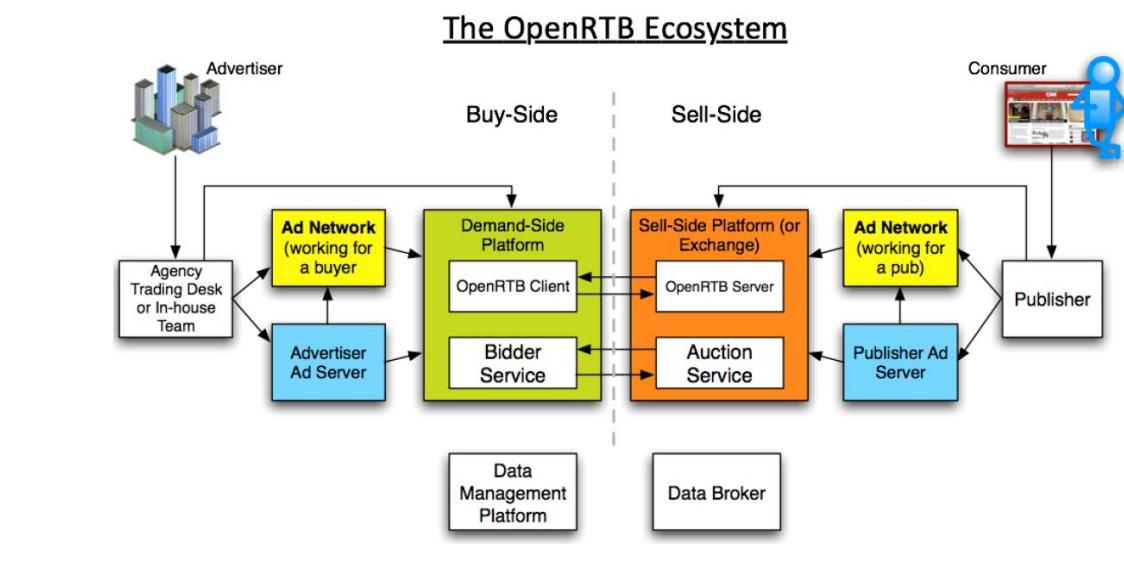
⁷ Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), p. 5.

using a DMP, an advertiser can enrich and combine data that it himself has about (potential) customers with data that it can get from a central DMP. Thus, one of the main functions of a DMP is to create detailed consumer profiles through data enrichment in order to optimise the targeting and effectiveness of marketing and advertising campaigns and to provide personalised offers on websites and in applications⁸.

25. After an advertiser has drawn up detailed consumer profiles via a DMP, it bids via its DSP for *bid requests* from publishers/SSPs offering advertising space that matches those consumer profiles.
26. In RTB jargon, SSPs, DSPs, Ad Exchanges, advertisers and DMPs are collectively referred to as "Vendors".
27. Schematically this can be presented as follows⁹:



28. This can also be represented as follows¹⁰:



⁸ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 7.

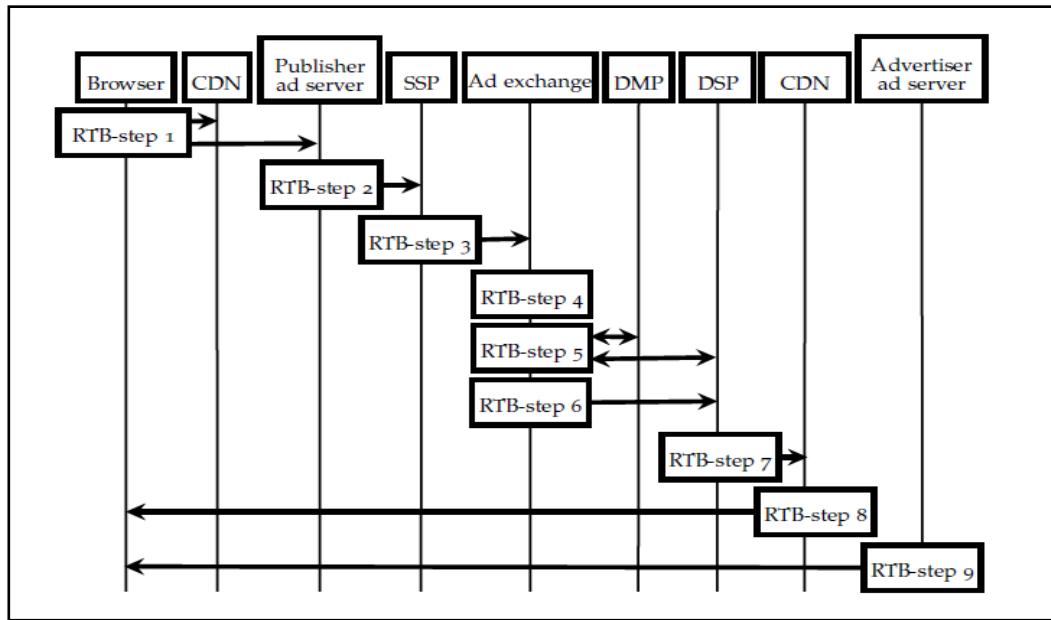
⁹ M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", German Law Journal, 31 July 2021, p. 9.

¹⁰ Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), p. 6.

29. The content of a *bid request*, which contains data about online users, their device and the websites visited, is captured by the OpenRTB system or the Authorised Buyers system. Generally, the following categories of personal data can be communicated in a *bid request* with advertisers¹¹:
- URL of the visited site
 - Category or subject of the site
 - Operating system of the device
 - Browser software and version
 - Manufacturer and model of the device
 - Mobile operator
 - Screen dimensions
 - Unique user identification set by vendor and/or buyer.
 - Unique person identifier from the Ad Exchange, often derived from the Ad Exchange's cookie.
 - The user identification of a DSP, often derived from the Ad Exchange's cookie that is synchronised with a cookie from the DSP's domain.
 - Year of birth
 - Gender
 - Interests
 - Metadata reporting on consent given
 - Geography
 - Longitude and latitude
 - Post code
30. As a result, it is beyond doubt that the GDPR applies *ratione materiae* to the RTB system, of which the OpenRTB protocol and, to some extent, the Transparency & Consent Framework (TCF) discussed below are essential components, as RTB operations by means of *bid requests* inherently entail the processing of personal data.
31. The different steps and interactions between the SSPs, DSPs and DMPs that take place in the RTB system can be summarised as follows¹²:

¹¹ *Ibidem*, p. 10.

¹² R. VAN EJK, "Web Privacy Measurement in Real-Time Bidding Systems- A Graph-Based Approach to RTB system classification", 2019, p.150-151, available at <https://ssrn.com/abstract=3319284>.



- i. An end user requests a web page;
 - ii. The *publisher's ad server* on the web page selects an SSP;
 - iii. The SSP then selects an *Ad exchange*;
 - iv. The *Ad Exchange* sends *bid requests* to hundreds of network partners and offers them the opportunity to generate a *bid response*;
 - v. The *Ad Exchange* allows privileged DMPs and/or DSPs to synchronise http cookies;
 - vi. The *Ad exchange* places the winning bid;
 - vii. The DSP serves the advertiser's ad;
 - viii. The ad is loaded from a *CDN* (Content Delivery Network, or network provider);
 - ix. The advertiser's server loads a Javascript for verification;
32. *Real-time bidding* poses a number of risks that stem from the nature of the ecosystem and the way personal data is processed within it. These risks include¹³:
- profiling and automated decision-making;
 - large-scale processing (including special categories of personal data);
 - innovative use or application of new technological or organisational solutions;
 - matching or merging of datasets;
 - analysis or prediction of behaviour, location or movements of natural persons;
 - invisible processing of personal data.

¹³ Information Commissioner's Office, "Update report into adtech and real time bidding", 20 June 2019, p. 9 - <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>

33. In addition, a large number of organisations — such as data controllers, joint data controllers, processors or other data subjects — are part of the ecosystem. This has a potentially significant impact on data protection. Moreover, most data subjects have a limited understanding of how the ecosystem processes their personal data.
34. As a result, the GDPR applies to the processing operations carried out within the framework of RTB, which are of such a nature that they can create a significant risk to the rights and freedoms of individuals.

A.3.2. - IAB Europe's Transparency & Consent Framework

35. IAB Tech Lab has developed the OpenRTB protocol, which together with Google's AdBuyers protocol, is the most widely used RTB protocol worldwide. IAB Tech Lab, based in New York in the United States of America, acts as a provider of the OpenRTB standard and should be distinguished from IAB Europe, which developed the Transparency and Consent Framework (TCF).
36. IAB Europe is a federation representing the digital advertisement and marketing industry on the European level. It comprises corporate members as well as national associations, with their own corporate members. Indirectly, IAB Europe represents approximately 5.000 companies, including both large corporations and national members¹⁴.
37. According to IAB Europe, the defendant in these proceedings, the TCF provides accountability and transparency to the OpenRTB. The TCF constitutes a separate set of policies, technical specifications, terms and conditions, created, managed and administered by IAB Europe, and, according to the defendant, should be capable of informing users of the legitimate interests pursued by advertisers, as well as obtaining the valid consent of those users with regard to the processing of their personal data in a real-time bidding system (such as OpenRTB).
38. Although the OpenRTB should be distinguished from the TCF, the two systems are connected. After all, IAB Europe claims that the TCF provides an operational framework in which the data processing operations that take place on the basis of the OpenRTB protocol can be brought in line with the GDPR (and the ePrivacy Directive).
39. In relation to the TCF, IAB Europe states the following:

"In its current form, the TCF is a cross-industry best practice standard that facilitates the digital advertising industry's compliance with certain EU privacy and data protection rules and seeks to bring improved transparency and control to individuals over their personal data. Specifically, it is a 'framework' within which businesses operate independently and which

¹⁴ As indicated by the CEO of the defendant during the hearing before the Litigation Chamber, on 11 June 2021.

helps them satisfy the requirement to have a GDPR legal basis for any processing of personal data and the requirement for user consent for the storing and accessing of information on a user device under the ePrivacy Directive.”¹⁵

40. Moreover, the main players within the TCF correspond to a large extent to the parties participating in the OpenRTB (with the exception of the Consent Management Platforms, i.e. ‘CMPs’):
 - i. Publishers— Parties who make advertising space available on their website or in their application and who are in direct contact with users whose personal data are collected and processed. A *publisher* may provide a CMP (see below) on its website or in its app to enable it to seek and manage the consent of visitors/users to the processing of their personal data and to facilitate the operation of TCF¹⁶. *Publishers* decide which *adtech vendors* may collect data through their website and process their users' personal data (and/or access their devices) and for what purposes¹⁷.
 - ii. Adtech vendors — Companies that receive personal data from *publishers* in order to fill advertising spaces on *publisher* websites or in publisher apps, such as advertisers, SSPs, DSPs, Ad Exchanges, and DMPs.
 - iii. Consent Management Platforms— Specifically for TCF, there are also companies that offer so-called "Consent Management Platforms" (CMPs). Specifically, a CMP takes the form of a pop-up that appears during the first connection to a website to collect the Internet user's consent to the placement of cookies and other identifying information¹⁸.
41. An essential part of the intervention of a CMP is the generation of a character string consisting of a combination of letters, numbers and other characters. This string is called the "TC String" by IAB Europe, which stands for the "Transparency and Consent String". The TC String is meant to capture in a structured and automated way the preferences of a user when he visits a website or app of a *publisher* that has integrated the CMP. This concerns in particular the capturing of consent (or not) to the processing of personal data for marketing and other purposes, whether or not to share personal data with third parties (*adtech vendors*) and the exercise or not of the right to object.
42. Vendors decipher the TC String to determine whether they have the necessary legal basis to process a user's personal data for the specified purposes. Thanks to its concise data

¹⁵Conclusions of the defendant's reply dated 25 March 2021, para. 32.

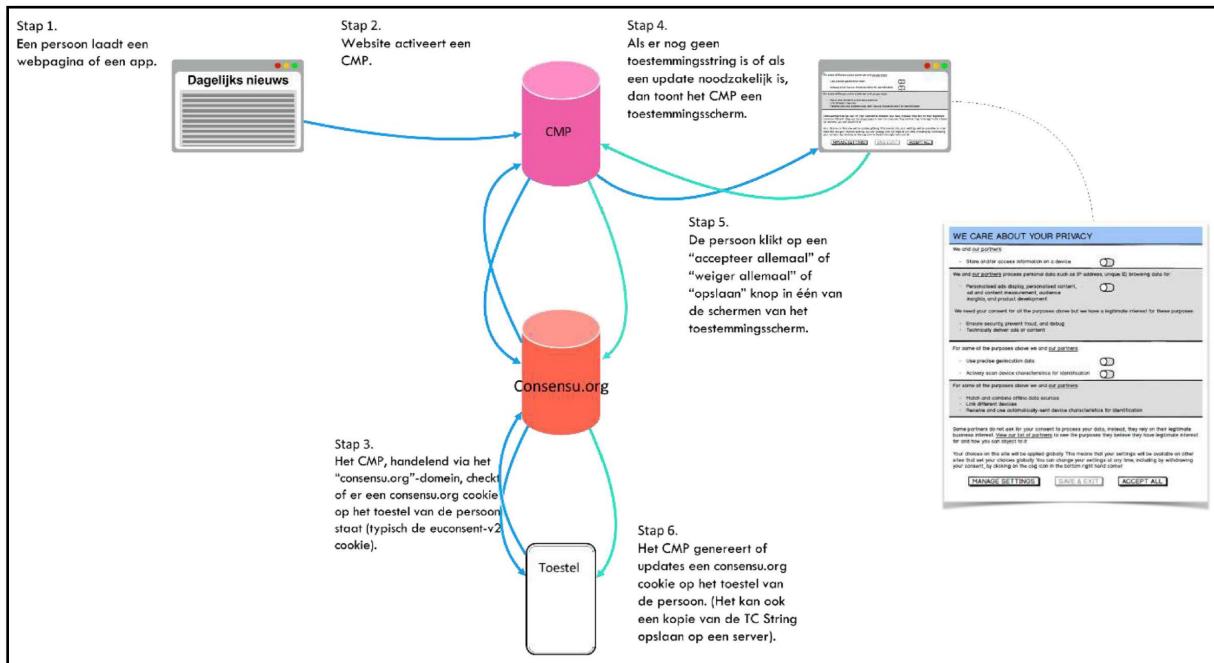
¹⁶ Information Commissioner's Office, "Update report into adtech and real time bidding", 20 June 2019, p. 11-12, <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>.

¹⁷Conclusions of the defendant's reply dated. 25 March 2021, para. 36.

¹⁸ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 59.

format, the CMP can store and retrieve a user's preferred data at any time and pass this information on to adtech vendors who need it¹⁹.

43. This can be represented schematically as follows²⁰:



- i. An Internet user browses the website of a *publisher*, for example a news website.
- ii. The *publisher* ensures that a CMP is activated on its website or in its app when the user arrives.
- iii. The CMP checks whether a TC String already exists for this user or not. If a "globally stored" TC String²¹ is chosen, the CMP will contact the IAB Europe-managed consensu.org internet domain to verify from there whether there is already a so-called "consensu" cookie on the user's device. In particular, this relates to the *euconsent-v2* cookie.
- iv. If the third step shows that the TC String does not yet exist or is not up to date, in a fourth step the CMP will show the user a user interface where he can consent to the collection and sharing of his personal data.
- v. The Internet user makes a choice in the user interface.
- vi. The CMP generates the *TC String* and places a *euconsent-v2* cookie on the user's device or updates the existing cookie.

¹⁹ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 75.

²⁰ Conclusions of the complainant dated 18 February 2021, para. 18.

²¹ Also referred to as "globally scoped consents".

A.4. - Reports of the Inspection Service

A.4.1 - IAB Europe acts as data controller in respect of the Transparency and Consent Framework and the personal data processing operations relating thereto

44. In these proceedings, the Inspection Service focused its investigation exclusively on IAB Europe, which the Inspection Service identified as the data controller for the TCF. The Inspection Service supports this initial finding with the fact that IAB Europe developed the TCF, with which IAB Europe imposes binding rules on participating organisations. According to the Inspection Service, these binding rules relate in particular to the processing of personal data in the context of the collection and processing of consent, as well as the preferences of online users, regarding processing purposes and authorised adtech vendors.
45. The Inspection Service bases its report on two technical analyses related to the *Open Realtime Bidding API Specification* of IAB Europe, as well as the different mechanisms under the *OpenMedia* specification of IAB Tech Lab, including the *Transparency and Consent Framework* developed by IAB Europe jointly with IAB Tech Lab²².
46. With regard to the OpenRTB protocol, the Inspection Service concludes that IAB Tech Lab, which developed this open technical standard and is based in New York (USA), merely acts as a provider of the system with respect to participating organisations and therefore cannot be considered a data controller. In contrast to the TCF, the OpenRTB allows the processing of personal data in accordance with means and purposes entirely determined by the participating organisations, but not by IAB Tech Lab.
47. Finally, the Inspection Service states that the Belgian DPA is not competent for the *Authorised Buyers* protocol, which was developed by Google as an alternative to the OpenRTB standard.

A.4.2. - Identified infringements of the GDPR

48. The Inspection Service finds that IAB Europe is in breach of the following legal provisions and principles of the GDPR with its *Transparency and Consent Framework*:
 - Articles 5.1.a and 5.2 (principles of fairness, transparency and accountability);
 - Article 6.1 (lawfulness of processing);
 - Article 9.1 and 9.2 (processing of special categories of personal data);
 - Article 12.1 (transparency of information, communications and modalities for exercising data subjects' rights);

²² Technical Analysis Reports of the Inspection Service, 4 June 2019 (Exhibit 24) and 6 January 2020 (Exhibit 53). Whereas IAB Europe drafted the TCF Policies, IAB Tech Lab developed the technical specifications in accordance with said Policies.

- Article 13 (information to be provided when personal data have been obtained from the data subject);
 - Article 14 (information to be provided when personal data have not been obtained from the data subject);
 - Article 24.1 (responsibility of the data controller);
 - Articles 32.1 and 32.2 (security of processing).
49. Outside the scope of the complaints, the Inspection Service also finds additional infringements of the following provisions of the GDPR:
- Article 30 (register of processing activities);
 - Article 31 (cooperation with the supervisory authorities);
 - Article 24.1 (responsibility of the data controller);
 - Article 37 (appointment of a data protection officer).
- Finding 1 - IAB Europe wrongly uses legitimate interest as a basis for processing personal data under the TCF, whereby special categories of personal data may also be processed in certain cases.
50. Based on the two versions of the *IAB Europe Transparency & Consent Framework Policies*²³, the Inspection Service notes that IAB Europe places the responsibility for compliance with the principles of transparency and fairness on the CMPs and/or publishers. Moreover, IAB Europe takes the position that the legitimate interest of participating organisations is an appropriate basis for processing personal data within the framework of the TCF in order to create an advertising profile of the data subjects and to display personalised advertising to them. However, according to the Inspection Service, IAB Europe fails to provide evidence that the interests, in particular the fundamental rights and freedoms, of data subjects were adequately considered in the process.
51. Incidentally, the Inspection Service notes that in certain circumstances, special categories of personal data may also be collected and processed by the participating organisations. For example, participating organisations could learn about the websites previously visited by a data subject, whereby the political opinions, religious or philosophical convictions, sexual orientation, health data or even trade union memberships of the data subjects could be inferred or revealed.
52. The Inspection Service considers that IAB Europe has thus failed to comply adequately with the principles of transparency and fairness in relation to the persons concerned.

²³ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

Finding 2 - The information provided does not comply with Articles 12.1, 13 and 14 of the GDPR

53. The Inspection Service also finds that the privacy policy that IAB Europe makes available to data subjects is not always transparent or understandable, which constitutes a breach of the obligations arising from Articles 12.1, 13 and 14 of the GDPR.
54. The privacy policy of IAB Europe²⁴ is available only in English. In addition, the privacy policy contains several terms that, without further explanation, are unclear to those involved. By way of example, the Inspection Service mentions "services" and "other means".
55. Moreover, according to the Inspection Service, the information provided is incomplete and inadequate. Firstly, data subjects are not informed of the exact legitimate interests pursued by IAB Europe. Secondly, it is not easy for data subjects to distinguish between the different recipients or categories of recipients of their personal data; the terms "*third parties*" and "*partners*" are not understandable without further explanation. Thirdly, data subjects are not informed, on the one hand, about the reference to appropriate or sufficient safeguards for the international transfer of their personal data outside the EEA or, on the other hand, about how to obtain a copy or where it is made available. Fourthly, based on the privacy policy of IAB Europe, it is not clear to data subjects that their personal data can be obtained by IAB Europe via its TCF²⁵. Fifthly, the conditions under which data subjects must provide their personal data, in particular whether this collection is organised on the basis of a legal, pre-contractual or contractual obligation, are not clearly set out. Nor are the data subjects informed of the possible consequences of not providing their data.
56. Therefore, the privacy policy does not comply with the obligations enshrined in Articles 13 and 14 of the GDPR.

Finding 3 - IAB Europe does not foresee any compliance control under the TCF policy rules

57. On the basis of the two versions of the *IAB Europe Transparency and Consent Framework Policies*²⁶, the Inspection Service is of the opinion that IAB Europe does not sufficiently monitor compliance with the rules it has developed with regard to participating organisations. In particular, it would be possible for a CMP to continue exchanging personal data with a publisher even if it reasonably considers that this Publisher does not comply with the rules imposed by IAB Europe in the context of its TCF or the rules imposed by the legislation²⁷.

²⁴ Exhibit 41.

²⁵ Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33), p. 7.

²⁶ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

²⁷ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 11 ; IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38), p. 6.

58. Given the role that IAB Europe assigns to itself, namely that of *Managing Organisation*, this disregard for the risks to the rights and freedoms of data subjects would indicate a breach of Article 24.1 GDPR as well as of the obligation to provide appropriate security for the processing of personal data, pursuant to Articles 32.1 and 32.2 GDPR.

Finding 4 - IAB Europe failed to keep a register of processing operations

59. The Inspection Service also notes that IAB Europe does not consider itself obliged to keep a register of processing activities, based on the exception provided in Article 30.5 GDPR for organisations with fewer than 250 persons²⁸. The Inspection Service also points out that IAB Europe did not initially provide a copy of its register of processing activities to the Inspection Service.
60. Only in a second reply²⁹ did IAB Europe decide, for the sake of completeness, to provide a register of processing activities, although the organisation still does not consider itself subject to the obligation under Article 30.5 GDPR.

Finding 5 - IAB Europe did not cooperate sufficiently with the investigation by the Inspection Service

61. Based on finding 4, and with reference to the delay with which IAB Europe responded to the Inspection Service's requests for additional information, the Inspection Service concludes that the conduct of IAB Europe in the context of its investigation is in breach of the duty to cooperate under Article 31 of the GDPR.

Finding 6 - IAB Europe failed to appoint a data protection officer, although as Managing Organisation it reserves the right to access the (personal) data that organisations participating in the TCF collect and process

62. IAB Europe asserts³⁰ that it does not fulfil the conditions referred to in Article 37.1.b of the GDPR, as "*IAB Europe is a professional association whose main activities are to provide information and tools to stakeholders (in particular, companies) operating in the digital advertising sector, as well as to provide information to the general public in order to improve their knowledge and to inform them of the value that digital advertising brings to the market*". For these reasons, IAB Europe has not appointed a data protection officer.
63. According to the Inspection Service, the approach of IAB Europe set out above is not supported by the facts. IAB Europe developed and manages the TCF in its capacity as *Managing Organisation* and as such, as well as under the terms and conditions of the IAB

²⁸ IAB Europe - Response to Belgium DPA, 26 June 2019 (Exhibit 22), p. 2-3.

²⁹ IAB Europe response to the Inspection Report, 10 February 2020 (Exhibit 57).

³⁰ In its reply to the Inspection Service dated 26/06/2019 and 20/08/2019, Exhibits 22 and 29.

Europe Transparency & Consent Framework³¹, has a right to access and to store and process all information provided by participating organisations.

A.4.3. - Additional considerations that the Inspection Service considers relevant to the assessment of the gravity of the facts

64. The Inspection Service refers to the judgment of the Court of Justice of the European Union (hereinafter "the Court of Justice") in Case C-25/17 (Jehovah's Witnesses)³², in which the Court clarified that the definition of data controller must be interpreted broadly in order to ensure effective and complete protection of data subjects. In this regard, the Inspection Service argues that IAB Europe is trying to evade its responsibility under the GDPR.
65. The Inspection Service refers to clauses included under Title 10 "*Liability*" of the General Terms and Conditions for the TCF³³, with which IAB Europe places the responsibility for the processing of personal data collected by the parties of the digital advertising sector entirely on the CMPs, publishers and other adtech vendors³⁴. Indeed, these clauses expressly state that IAB Europe does not guarantee in any way that:
 - the consent given by CMPs or *publishers* to authorised partners (*global adtech vendors*) has been collected and processed in accordance with, *inter alia*, the GDPR;
 - any data processing carried out in connection with, or on account of, the TCF shall comply with all relevant laws and regulations, including the GDPR.

A.5. - Summary of the defendant's response dd. 11 February 2021

A.5.1. - IAB Europe is not a data controller with regard to the processing of personal data in connection with the TCF

66. The defendant refutes the Inspection Service's view that it acts, in its capacity as *Managing Organisation*, as a data controller in respect of the personal data processed by participants in the Transparency and Consent Framework.
67. According to the defendant, the TCF in no way obliges the participating organisations to pursue certain objectives, but merely aims to provide the information, which must be provided to data subjects in accordance with Articles 12 and 13 of the GDPR, in a

³¹ Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33).

³² CJEU judgment of 10 July 2018, C-25/17, Jehovah's Witnesses, ECLI:EU:C:2018:551.

³³ Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33).

³⁴ In particular, the *Supply-Side Platforms*, *Demand-Side Platforms*, *Ad Exchanges*, *Advertisers* and *Data Management Platforms*.

streamlined and standardised manner by means of the CMPs. In contrast, the actual processing purposes are determined by the participating organisations, without the intervention of the defendant.

68. Firstly, the defendant addresses the lack of legal capacity (*ratione personae*) on the part of the DPA, and more specifically the Inspection Service, to conduct an investigation and to challenge the TCF. The defendant also refers to the DPA's capacity to hold the actual data controllers, i.e. the participants in the TCF, accountable for possible infringements of the GDPR, where necessary.
69. According to the defendant, the TCF as such does not entail any processing of personal data and the Inspection Report does not show for which processing activities IAB Europe should be regarded as the data controller.
70. Secondly, it argues that a broad definition of the concept of a data controller, as proposed by the Inspection Service, is not justified in the context of the TCF, since there are already clearly identified data controllers, on the one hand, and in view of the fact that the TCF has no influence on the processing of personal data that takes place in the context of the OpenRTB protocol, on the other. More specifically, the defendant refers to the lack of any influence on both the means and ends of processing within the RTB system.
71. The defendant also considers that the Jehovah's Witnesses judgment cited above does not apply to the situation of IAB Europe, for the following reasons:
 - Unlike the Jehovah's Witness Community, IAB Europe does not "organise, coordinate or promote" in any way the processing of personal data by TCF participants.
 - The processing of personal data by TCF participants for RTB purposes is not in the interest of IAB Europe.
 - TCF participants have no common purpose in processing personal data and only participate in the TCF with the aim of achieving their individual objectives in a manner that is compliant with the GDPR.
72. The defendant is of the opinion that the *Wirtschaftsakademie*³⁵ ruling does not apply to IAB Europe either, as the defendant never disseminates information (i.e. advertising) on behalf of or at the behest of advertisers; does not choose an advertising platform or other communication channel; and does not set any parameters or processing purposes, unlike the participants in the TCF who do decide on these matters. According to the defendant, IAB Europe is not actively involved in any RTB processing and it does not initiate such

³⁵ CJEU judgment of 5 June 2018, C-210/16, *Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388.

processing in any way or form. The data processing associated with the OpenRTB system is carried out exclusively by TCF participants and therefore takes place independently of IAB Europe or the TCF.

73. Thirdly, it discusses the definition of a data controller as explained in guidelines issued by the European Data Protection Board (EDPB).³⁶ The defendant claims that it does not exercise any discretion as to the purposes or means of the processing of personal data within the framework of the TCF. Furthermore, IAB Europe does not process personal data in a way that could be regarded as "inseparable" from, or "inextricably linked" to, the processing of personal data by participants in the TCF. Also, the fact that participating organisations pay a financial fee to IAB Europe does not constitute, according to the defendant, a "mutual benefit" that would lead to a joint processing responsibility.
74. Moreover, the defendant emphasises the lack of decisions or guidelines from other supervisory authorities which could support the Inspection Service's view. In particular, the Belgian, German, French and UK supervisory authorities failed to identify IAB Europe as a (joint) data controller. Specifically, the Conference of Independent Data Protection Authorities of the German Federation and the Länder decided in September 2019 that IAB Europe was acting purely as a representative organisation in the sector of programmatic advertising. In addition, the German supervisory authorities confirmed their position in November 2019, when they announced that any enforcement proceedings related to complaints against online advertising should be initiated against TCF participants, but not against IAB Europe. According to the defendant, the French supervisory authority (CNIL) also indirectly accepted the view that IAB Europe was not responsible for the processing operations carried out by participants in the TCF. Also, the UK ICO has allegedly never identified IAB Europe as a potential data controller within the RTB ecosystem at any point.
75. Finally, the defendant refers to the possible consequences for other organisations subject to the GDPR if the Litigation Chamber were to rule that IAB Europe is indeed (co-)responsible for the processing of personal data within the framework of the TCF. In particular, according to the defendant, such a decision would mean that any umbrella organisation which develops and adopts a code of conduct would, merely by virtue of its supervisory role, be deemed to be co-responsible with regard to the processing operations carried out by other organisations in accordance with that code of conduct.

³⁶ EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021.

A.5.2. - The TCF complies with the GDPR

a. Legality and legal basis

76. First of all, the defendant argues that IAB Europe, unlike the participating organisations, is not at all obliged to explain to the Inspection Service the existence of a legitimate interest, including a balancing of the interests of participating organisations against the rights and freedoms of data subjects, since IAB Europe does not participate in the TCF nor does it act as a data controller.
77. Moreover, the defendant claims that the DPA is not authorised to prohibit participants in the TCF from processing personal data of data subjects on the basis of a legitimate interest. On the contrary, the assessment of the merits of the legitimate interests asserted by the participants must be made on a case-by-case basis, and therefore cannot be prohibited in advance and in absolute terms by the DPA.
78. As regards the allegations that IAB Europe processes special categories of personal data within the framework of the TCF, or is allegedly jointly responsible for the processing of such personal data by the participating organisations, the defendant points out that such categories of personal data may, if necessary, only be processed within the framework of the OpenRTB, as opposed to the TCF. The defendant refers in this regard to the TCF Policies, which expressly prohibit the use of the TCF to process special categories of personal data.

b. Transparency

79. In view of the fact that IAB Europe does not act as a data controller in respect of personal data processed for RTB purposes, the defendant argues that it cannot be expected to inform data subjects in accordance with Articles 12 and 13 of the GDPR either.
80. Moreover, the defendant claims that the privacy policy which the Inspection Service invokes as evidence of possible infringements of the principle of transparency is applicable exclusively to the processing of personal data collected on the various websites operated by the defendant, as well as to the personal data collected in connection with the participating organisations (in particular, the contact details of representatives of those organisations). In other words, the privacy policy to which the Inspection Service refers has no connection whatsoever, according to the defendant, with the processing activities in the context of the OpenRTB system.
81. The defendant also disputes any allegation that IAB Europe, in its capacity as Managing Organisation, reserves the right to access the personal data collected and exchanged by the participating organisations within the framework of the TCF and the OpenRTB system. IAB Europe claims that this assumption is not based on any evidence and is due to an

incorrect interpretation of the possibility offered to the defendant to process personal data of representatives of participating organisations.

82. Moreover, the defendant considers that it is entitled to offer the privacy policy exclusively in English, since the target audience is mainly professional, B2B actors. The defendant points out that Belgian law does not provide for any obligation to make a privacy policy available in French or Dutch and that, moreover, Belgium has failed to make use of the possibility of adopting additional requirements concerning the use of language within the framework of the European Directive on consumer rights³⁷.

c. Security

83. The defendant claims that the charges concerning the lack of technical and organisational measures to protect personal data in connection with the TCF are unfounded.
84. First of all, the defendant takes the view that IAB Europe is not subject to Articles 24 and 32 of the GDPR in respect of the data processing operations carried out within the TCF, as the organisation is not a data controller.
85. Secondly, the Transparency & Consent Framework Policies provide that participants in the TCF must report infringements of TCF rules to IAB Europe. Again, the defendant claims that the Inspection Service is misinterpreting the TCF Policies, in particular by granting CMPs the right to terminate the cooperation if they consider that a publisher does not comply with the rules, without suffering any contractual disadvantage. In addition, the defendant notes that infringements of the rules provided for in the TCF can always be reported to the supervisory authorities, which will then take action if they deem it necessary.

d. International transfer of personal data

86. IAB Europe refutes the complainants' allegations concerning the international transfer of personal data within the framework of the TCF. The defendant notes in this regard that these allegations are only relevant in the context of the OpenRTB system, which is not at issue in this case. Incidentally, IAB Europe cannot be held responsible for the transfer within the framework of the OpenRTB System.

A.5.3. - IAB Europe is not subject to the obligation to keep a register of processing operations

87. The defendant emphasises that it can invoke the exception provided for in Article 30.5, in particular that the organisation does not have to keep a register of processing activities, as

³⁷ Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ L 304/64.

IAB Europe is not a data controller in respect of the processing activities carried out within the TCF and, moreover, the organisation has fewer than 250 employees. Nevertheless, the defendant emphasises its own initiative in drawing up a register and submitting it to the Inspection Service, as well as the fact that this register does not relate to processing activities relating to the TCF.

A.5.4. - IAB Europe is not required to appoint a data protection officer

88. Having regard to the nature and scope of the processing activities carried out by the organisation, the defendant states that IAB Europe is not required to appoint a data protection officer, since the criteria laid down in Article 37 of the GDPR are not met.

A.5.5. - IAB Europe did cooperate with the Inspection Service

89. The defendant refutes the allegations of insufficient cooperation with the investigation, noting that the time limits imposed by the Inspection Service on parties to an investigation are in no way determined by law, but must be the result of reasonable assessment and must take into account the specific circumstances of the case. *In the present case*, the defendant takes the view that IAB Europe has always cooperated in good faith and provided information and replies in an attempt to clarify its status in relation to the TCF and to demonstrate its compliance with the GDPR, in so far as it applies to IAB Europe.
90. In addition, the defendant observes that the duty of cooperation under Article 31 of the GDPR cannot in any way be construed as an obligation to provide documentation in accordance with provisions of the GDPR which the defendant does not consider to be required.

A.5.6. - There are no aggravating circumstances to the detriment of IAB Europe

91. Finally, IAB Europe disputes the Inspection Service's finding that the defendant's denial that IAB Europe is acting as a data controller, as well as the large volume of both personal data processed and of participating organisations, may be regarded as aggravating circumstances.
92. The defendant refers to the lack of clear evidence in the investigation report that these circumstances are aggravating and concludes that the allegations are due to insufficient knowledge of the operation of the TCF. Consequently, the defendant requests the Litigation Chamber to disregard the opinion of the Inspection Service.

A.6. - Summary of the complainants' reply submissions dd. 18 February 2021

A.6.1. – IAB Europe is data controller for the TCF

a. Processing of personal data within the framework of the TCF

93. The complainants argue that a unique identification number, such as the TC String generated and stored in a cookie, is personal data within the meaning of Article 4(1) of the GDPR, a position which has also been expressly confirmed in case law prior to the GDPR.
94. Moreover, according to the complainants, the TC String is more than just a unique identifier, as IAB Europe allegedly also uses the TC String to collect information regarding which applications a data subject uses and which websites he visits. This could also reveal sensitive data on data subjects within the meaning of Article 9 of the GDPR.
95. Furthermore, the generation of the TC String in itself constitutes, without any doubt, processing of personal data. The issue at hand is the automated creation, by a CMP registered with the TCF, of a unique and linked set of characters intended to capture a specific user's preferences regarding permitted data exchanges with advertisers.
96. The sharing of the TC String with CMPs takes place, according to the complainants, in two ways:
 - a. storing the TC String in a shared *globally scoped consent* cookie on the IAB Europe *consensu.org* internet domain; or
 - b. storing the TC String in a storage system chosen by the CMP if it is a service-specific permission.
97. According to the complainants, in both cases IAB Europe is the data controller of those processing operations. The intervention of IAB Europe is, moreover, all the more drastic in the hypothesis of the shared *global consent* cookie. Indeed, that shared *globally scoped consent* cookie that stores the TC String points to the "*consensu.org*" domain, managed by IAB Europe, from where CMPs can access and update the shared TC String.

b. IAB acts as data controller for the processing operations within the TCF

98. First of all, the complainants believe that IAB Europe, in its "*Frequently Asked Questions*" about the TCF, explicitly states that it is responsible for the *TCF Policies*.
99. According to the complainants, it goes without saying that the organisation that manages and operates the TCF is also the data controller of this system, including any processing of personal data imposed and organised by the TCF. After all, IAB Europe imposes these personal data processing operations on the other participants in an enforceable manner.
100. Furthermore, IAB Europe requires CMPs to implement the TCF strictly according to its *Technical Specifications*. In the *TCF Technical Specifications*, IAB Europe explains in detail

which personal data must be processed by the participants, for what purposes and by what means.

101. IAB Europe also requires CMPs, in the case of a global consent, to store the character string in a shared *global consent* cookie on the "consensu.org" domain. Since this internet domain is registered and managed by IAB Europe, the defendant also has access to the personal data processed in the TCF.
102. Moreover, according to the complainants, IAB Europe determines the so-called "essential means" for the processing of personal data within the TCF. On the one hand, IAB Europe specifies in detail which elements must be included in the TC String. And, on the other hand, IAB Europe determines the categories of recipients of that personal data, as the defendant is responsible, in its own words, for the management of the *Global Vendor List* and the management of the CMPs participating in the TCF.
103. The complainants also believe that TCF does not provide an effective mechanism to enforce certain policies³⁸, although a code of conduct is intended to be an effective system for compelling its members to comply, as stipulated in Article 41 GDPR.

A.6.2. - The processing operations carried out in the TCF violate the GDPR at various levels

a. Infringement of the principles of purpose, proportionality and necessity

104. According to the complainants, IAB Europe collects users' preferences in the TCF via the TC String for a vague, inaccessible and abusive purpose, while the personal data processed is insufficient and irrelevant for this purpose.
105. Moreover, the processing in itself is alleged to be anything but proportionate, which means that IAB Europe is in breach of Articles 5(1)(b) and 5(1)(c) of the GDPR, as well as its duty of responsibility as the data controller, laid down in Article 5(2) of the GDPR. Furthermore, the complainants consider that, with the design of the TCF, IAB Europe does not provide the necessary guarantees for compliance with the requirements of the GDPR and for the protection of the rights of data subjects; consequently, the defendant infringes Article 25 GDPR.

The purpose of processing the TC String is neither specified nor explicitly defined for data subjects, nor is it justified

106. According to the complainants, IAB Europe does not provide information to data subjects concerning the processing of their personal data in the TCF.

³⁸ See para. 133 et seq. of this decision.

107. The purpose of the TC String within the overall purpose of the TCF is to capture the information provided to users and their processing preferences. In other words, IAB Europe does process personal data (in particular the TC String) within the TCF because it claims this could bring the underlying marketing-related processing in line with the GDPR. According to the complainants, it is therefore this purpose that must be assessed in terms of its lawfulness, and in the light of this purpose, the proportionality and necessity of the TC String's processing within the TCF must be assessed.

The TC String is inadequate and not relevant for the intended purpose

108. The complainants further argue that the TC String's processing operations within the TCF are insufficient and not relevant to ensure compliance with the GDPR when personal data are processed through the OpenRTB system.
109. The OpenRTB system contains an inherent security problem that makes it impossible for a system such as the TCF to guarantee, among other things, the necessary transparency and accountability with regard to personal data, including special categories of personal data, processed in a bid request after the bid request has been sent out.
110. The central idea behind the TCF is that participants collect user preferences and transmit them in the form of the TC String, so that other participants take note of the content (i.e. read the TCF signal) and can therefore respect the user preferences. However, according to the complainants, there is nothing in the TCF, or in any related system or mechanism, that actually ensures that participants in the OpenRTB system are bound by the TCF signal. The TCF signal is therefore no more than a mere notification.
111. Given the inherently unlawful nature of processing personal data in the OpenRTB system, on the one hand, and the inherently imperfect nature of a purely signal-based system such as the TCF without effective control, on the other, the use of the TCF, including the processing of the TC String, can never give participants the assurance of being in compliance with the GDPR. After all, the TCF offers no guarantee whatsoever that TCF participants will comply with their accountability obligations (Article 5.2 of the GDPR). Nor can it provide adequate protection for the personal data shared through the OpenRTB system (Article 5.1.f GDPR).

IAB Europe set up the TCF in such a way that data protection by design is not guaranteed

112. The complainants argue that the design of the TCF, due to its disproportionate nature, cannot guarantee the level of data protection required under Article 25 GDPR, in particular in view of the obligation arising from Article 25 GDPR to implement appropriate technical and organisational measures to ensure that, in principle, only personal data that are necessary for each specific purpose of the processing are processed.

113. The processing of personal data within the TCF, in particular the TC String, is therefore not necessary for the specific purpose as, according to the complainants, that purpose cannot and will not be achieved in any case.
114. Moreover, the complainants argue that the TC String, as an independent personal data that uniquely identifies users, is shared with numerous participants through various mechanisms, including through IAB Europe's own mechanism of the shared *global consent* cookie on its "consensu.org" internet domain.

b. Infringement of the principles of fair, lawful and transparent processing (Articles 5, 6, 12, 13 and 14 GDPR)

115. The complainants allege that data subjects are not informed in any way of the fact that their personal data (including the TC String) are systematically and widely processed by IAB Europe within the TCF.
116. According to the complainants, the processing of the personal data of the complainants and other data subjects by IAB in the TCF is after all:
 - anything but lawful as there is no legal basis;
 - neither proper nor transparent, as it takes place entirely "behind the backs" of those affected, without any form of notification.

IAB Europe's processing operations lack a legal basis and are therefore unlawful

117. IAB Europe cannot rely on the consent of data subjects (Article 6.1.a GDPR), according to the complainants, as it never sought or obtained such consent. Also nowhere in the *TCF Policies, Technical Specifications* or General Terms and Conditions is a mechanism cited whereby IAB Europe would ask data subjects for permission to generate a unique identifying string of characters that shares their privacy preferences with a mass of recipients, even in cases where those data subjects indicate in a CMP that they do not wish to share personal data with anyone.
118. According to the complainants, IAB Europe also cannot invoke the necessity of the processing of the TC String within the TCF for the performance of a contract with the complainants and other data subjects (Article 6.1.b), as there is no contract between data subjects and IAB Europe.
119. Furthermore, the complainants argue that the defendant may also not rely on the necessity of the processing of the TC String within the TCF to serve its legitimate interests, or those of a third party (Article 6.1.f GDPR). The required balancing of interests would always be in favour of those affected.
120. First of all, the processing of the TC String does not benefit the data subjects in any way as the TCF is not able to guarantee security, accountability or transparency. Moreover, there

is no legitimate interest, as this interest is not sufficiently clearly articulated anywhere, and it is not possible to balance it against the interests and fundamental rights of the data subjects.

121. Secondly, in balancing the interests, the data controller must in principle take into account several factors: the effects of the processing on the data subject, the nature of the personal data processed, the way in which these personal data are processed, the data subject's reasonable expectations, and the status of the data controller and the data subject.
122. According to the complainants, the consequences of the processing of the TC String are particularly far-reaching for those involved. IAB Europe's processing operations would lead TCF participants to assume that they are correctly informing data subjects about the processing of personal data through the OpenRTB system, but this is not the case. This would then lead to the unlawful sharing and distribution of personal data, even sensitive personal data, on an immense scale via the OpenRTB system.
123. IAB Europe's processing of the TC String would result in a unique online identifier being shared with untold numbers of parties, similar to what happens with unique identifiers in advertising cookies from large advertising companies. It would therefore allow easy tracking of users across the web and across devices ("*web and cross-device tracking*"). Moreover, the complainants argue that the TC String can be combined with the data distributed via the OpenRTB system, because the TC String is integrated in a *bid request*.
124. Given the lack of information for data subjects about the processing operations within the TCF and the unrestricted sharing of the TC String with an almost unlimited group of recipients, it is clear to the complainants that these processing operations are beyond the scope of the data subjects' reasonable expectations. Furthermore, data subjects such as the complainants do not expect that the processing of personal data within the TCF will result in their, sometimes sensitive, personal data and detailed profiles being shared with numerous companies through the OpenRTB system without any real and effective control over what those companies will do with the personal data obtained.
125. The complainants in this case are natural persons and interest groups representing the data protection interests of natural persons. They have no control over the processing of personal data within a TCF (which happens anyway, regardless of whether consent is given or refused in a CMP). Nor do they have control over what happens to their personal data shared through the OpenRTB system. According to the complainants, those involved cannot verify whether participants in OpenRTB actually comply with the rules of the TCF.

IAB Europe processes personal data in the TCF covertly without any form of notification and the processing is therefore neither proper nor transparent

126. Despite the extensive documentation that IAB Europe makes available to TCF participants on its website, nowhere does it state that the TCF itself also involves the processing of personal data, according to the complainants. Moreover, the documentation expressly disregards, with regard to TCF participants, that the TCF itself involves the processing of personal data.
127. The TCF Implementation Guidelines seems to suggest that there are hypotheses in which participation in a TCF does not involve the processing of personal data. After all, advertisers and DSPs, who already participate in the TCF, are told that they should register as vendors if they process personal data. According to the complainants, this implies that they would not have to do so if they were not processing personal data. However, the latter situation is entirely impossible, according to the complainants, as the TCF inherently requires the processing of personal data.
128. According to the complainants, the statements in the IAB Europe guidelines are misleading for the hundreds of *adtech vendors* who use TCF. Because IAB Europe does not inform TCF participants about the processing of personal data necessarily entailed by the implementation of a TCF, none of these participants knows or realises that they have a transparency obligation. In this way, data subjects - such as the complainants - are not informed by any participant of the processing of personal data within TCF.
129. IAB Europe does also not comply with its own transparency obligation. Neither on its own website nor in other sources does the defendant communicate the information required by Articles 13 and 14 to those concerned, such as the complainants. This would include the following information: that IAB Europe is the data controller of the TCF and its contact details; the contact details of its data protection officer; what its processing purposes are and the legal basis for the processing; which categories of personal data it processes (in particular the TC String); who receives the personal data (these are already at least all participants in the TCF who receive the TC String); that IAB Europe intends to transfer the personal data to recipients in third countries; how long the personal data are retained; what its legitimate interests for processing are; what the rights of the data subjects are; that data subjects may lodge a complaint with the DPA; that data subjects may withdraw their given consents; and finally, what the source of the personal data is.
130. At the same time, IAB Europe cannot invoke any of the exceptions provided for in Article 14.5 of the GDPR in order not to have to provide this information, as:
 - a. the data subjects are not yet in possession of the information, since the processing in respect of them has so far been carried out in secret (Article 14.5.a GDPR);

- b. it is not impossible nor does it require a disproportionate effort to make this information known to the data subjects, given the influence that IAB Europe exercises over the operation of the TCF (Article 14.5.b GDPR);
- c. the acquisition of these data is not prescribed by law (Article 14.5.c of the GDPR); and
- d. the personal data need not remain confidential for reasons of professional secrecy (Article 14.5.d GDPR).

IAB Europe's reference to the Vectaury case in France does not hold water

131. According to the complainants, IAB Europe wrongly believes that it can rely on the decision of the French supervisory authority CNIL in the Vectaury case. Indeed, IAB Europe wrongly claims that it would be strange for the Inspection Service to find infringements related to the processing of personal data in the TCF, while the CNIL is alleged to have no problems with the legitimacy of these processing operations. The complainants argue that IAB Europe is making assumptions here and reaching conclusions that cannot be deduced from the Vectaury case at all:
- Firstly, the Vectaury case was about the specific implementation of a CMP by Vectaury whereby the TCF would have been implemented. The role of IAB Europe was not the subject of those proceedings and CNIL therefore did not rule on, nor investigate, the role of IAB Europe in providing the TCF.
 - Secondly, that case specifically concerned whether Vectaury's implementation of the TCF could bring the underlying processing of real-time bidding systems in line with the GDPR. The CNIL's verdict was clearly negative, as shown by the fact Vectaury itself states on its website that it has created a completely new method in dialogue with the CNIL. According to the complainants, it is therefore misleading of IAB Europe to claim that the CNIL has legitimised the TCF in itself as being sufficient to bring real-time bidding systems into compliance with the GDPR.
 - Thirdly, the complainants argue that the CNIL investigation did not focus on the legitimacy of the processing of personal data within the TCF. The CNIL did not look at the generation and distribution of the TC String as a stand-alone processing and therefore did not make any statement about it.
132. According to the complainants, the CNIL's decisions in the Vectaury case are therefore irrelevant, as it was a clearly different case, directed against a different party, involving different processing operations and under legislation that has since been replaced. The Litigation Chamber follows the position of the complainants and does not discuss the Vectaury case, which concerns a different case than the present one.

c. Infringement of the principles of integrity and confidentiality (Articles 5.1.f and 32 of the GDPR)

133. According to the complainants, IAB Europe violates the integrity and confidentiality obligations of the GDPR because it facilitates the exchange of personal data in the TCF, in particular the exchange of the TC String, with numerous parties, without verifying whether all recipients of this personal data comply with the rules of the GDPR.
134. It is certain that the TC String is shared with thousands of companies. The TC String must therefore be protected by appropriate measures in accordance with Articles 5.1.f et 32 GDPR. However, IAB Europe has not built in an appropriate protection mechanism: As with all other processing in the OpenRTB system, there is no way to verify that recipients are effectively processing the TC String in accordance with the GDPR. Indeed, none of the mechanisms presented by IAB Europe is based on real, proactive control of TCF compliance, the complainants argue.
135. The complainants dispute IAB Europe's argument that it has no obligation to enforce the TCF, and in particular the agreements made within the TCF. The complainants argue that it is indeed its obligation as a data controller to enforce the agreements within the TCF and, at least in this way, to provide certain guarantees for the secure processing of the TC String.
136. Secondly, the complainants point to claims by IAB Europe that, as a management organisation, it makes "substantial efforts" to enforce the agreements within the TCF. According to the complainants, there is no evidence of these alleged "substantial efforts". They further argue that IAB Europe would have to verify each registered TCF participant's compliance with all agreements, which given the scale of data processing would imply a huge investigation. Moreover, the complainants refer to the answer given by IAB Europe itself to the Inspection Service: "*The reporting obligation itself is not currently monitored. Moreover, it is difficult to monitor it because it would be difficult for IAB Europe to establish whether or not or when a CMP had (or should have had) a "reasonable belief" that another party was not complying*"³⁹.
137. Thirdly, the complainants believe that IAB Europe is wrong to try to hide behind the contractual arrangements. According to the complainants, the defendant claims that it is sufficient that participants are contractually obliged to report any non-conformity to IAB Europe.
138. The complainants also argue that IAB Europe, as the data controller of the TCF, is bound by Articles 5.1.f and 32 of the GDPR, although it is practically impossible to guarantee the security of the processed TC String when it is shared with thousands of recipient

³⁹ Letter from IAB Europe to the Inspection Service of 10 February 2020, p. 8.

companies. According to the complainants, the latter would mean that IAB Europe actively checks that all recipients of the TC String always comply with the obligations of the GDPR so that the processing of the received TC String would not be unlawful.

139. Moreover, according to the complainants, practice proves that almost all participants in the TCF unlawfully process the TC String, as not one CMP, not one publisher and not one vendor provide information on the processing of the TC String, its purpose, legal basis or the categories of recipients. This would imply, according to the complainants, that the transfer of the TC String to these parties is inherently a personal data breach which, given its immense scale, gives rise to an obligation to report to the supervisory authorities.
140. The practical impossibility of providing the necessary safeguards for the protection of the personal data (in particular the TC String) of data subjects, when shared with thousands of recipients within the OpenRTB system, shows, according to the complainants, that IAB Europe is in breach of its obligations under Articles 5.1.f and 32 GDPR.

d. The systematic transfer of the TC String to third countries without adequate protection (breach of Article 44 of the GDPR)

141. The complainants argue that IAB Europe has set up the TCF in such a way that personal data — including the TC String, because it is integrated into the *bid requests* — is structurally transferred in the context of OpenRTB to numerous companies outside the European Economic Area (EEA), without adequate protection being provided for these transfers.
142. The complainants refer to the Ad Exchange Xandr (based in the USA), which is affiliated to IAB Europe's TCF and therefore receives at least the TC String from EEA users, including the complainants. As data controller for the processing of personal data in the TCF, IAB Europe should provide a mechanism for the transfer of personal data so that Ad Exchanges established outside the EEA may receive the TC String.
143. Exchanges of the TC String via real-time bidding systems such as OpenRTB are structural in nature and repeat themselves continuously in fractions of seconds. After all, the TC String is sent along with the *bid requests*. This would make it impossible for IAB Europe, according to the complainants, to invoke any of the exceptions in Article 49 GDPR.
144. Appropriate safeguards would be the only way for IAB Europe to organise transfers of personal data in the TCF. However, at present IAB Europe does not provide any form of appropriate safeguards for the transfer of the TC String through real-time bidding systems such as OpenRTB.

145. In line with the Schrems II judgment, IAB Europe,⁴⁰ in addition to selecting a form of adequate safeguards, should also have taken additional measures to prevent personal data from being processed in a non-compliant manner in third countries. However, these additional measures are just as lacking as appropriate safeguards. The TC String is shared in a blind manner with an indefinite number of participants in the OpenRTB system, wherever in the world they may be located.

A.7. - Summary of the defendant's rejoinder dd. 25 March 2021

A.7.1. - Organisations that process personal data within the RTB system are responsible for complying with the GDPR and the ePrivacy Directive

146. The defendant first argues that any party participating in RTB and using the OpenRTB specification can intervene in the technical storage and/or access operations on a user's device (e.g. the placing of website cookies) under the ePrivacy Directive, and/or act as a data controller or processor of personal data (e.g. for digital advertising purposes) under the GDPR. Where appropriate, all of these parties are responsible for complying with their obligations under the GDPR and the ePrivacy Directive when engaging in RTB.
147. In addition, according to the defendant, there are thousands of companies engaged in RTB and using the OpenRTB specification, which, however, do not participate in the TCF. Similarly, parties may use the TCF for purposes other than RTB. IAB Europe also stresses that publishers can use the TCF for a range of online advertising scenarios other than the OpenRTB specification - including other types of RTB protocols, but also online advertising that does not involve RTB at all, such as the direct sale of advertising inventory.
148. The defendant also refutes the complainants' allegations that RTB is inherently illegal by referring to the UK supervisory authority's (ICO) report which merely stated that RTB "requires organisations to take responsibility for their own data processing, and that the industry is collectively reforming RTB". The ICO is also said to have highlighted the good faith efforts of stakeholders such as IAB UK to contribute to this reform process in a more recent publication⁴¹.
149. Furthermore, the defendant states that several supervisory authorities have called for ways to increase transparency for data subjects by clearly identifying the data controllers with whom personal data will be shared, by specifying the processing purposes and by enabling

⁴⁰ CJEU judgment of 16 July 2020, C-311/18, *Facebook Ireland and Schrems*, ECLI:EU:C:2020:559.

⁴¹ Information Commissioner's Office - Adtech - the reform of real time bidding has started and will continue, 17 January 2020, <https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/>.

data subjects to exercise control over their personal data. It is precisely this kind of transparency measure that IAB Europe and the TCF aim to support.

150. Within the framework of the TCF, data subjects are given the opportunity to give their prior approval to a number of identified third parties (*adtech vendors*) and processing purposes. According to IAB Europe, this transparency and prior checking is an appropriate substitute, from a legal compliance perspective, for *real-time, on-the-fly*, one-by-one consent for access, storage and data processing by data controllers.

A.7.2. - IAB Europe cannot be held responsible for the alleged illegal practices of RTB participants, as the TCF is completely separate from RTB

151. The defendant emphasises that the TCF is only one of many optional approaches that data controllers may choose to help ensure compliance with transparency and consent requirements when processing personal data for RTB or other advertising purposes. Consequently, the responsibility for compliance and for the actual decisions on the purposes and means of these personal data processing operations lies entirely with the parties engaged in RTB, and not with IAB Europe.
152. The defendant also states that IAB Europe had contact with several supervisory authorities after the roll-out of the first version of the TCF, as well as with several *publishers*. Following these discussions, the second version of the TCF was developed, in which several processing purposes were bundled under one title in so-called "stacks", and the legitimate interest was introduced as a possible legal basis. Furthermore, the TCF v2 introduces additional purposes and "*publisher controls*" that allow publishers to restrict access to a particular purpose to a subset of *adtech vendors*.
153. Finally, the defendant clarifies that IAB Europe has always intended to have the TCF adopted as a transnational code of conduct.
154. In its initial submission, the defendant puts forward procedural arguments concerning the competence of the DPA and the way in which the complaints and the investigation were handled. These defences are set out below in Section A.9.
155. In its summary submission, the defendant also claims that the manner in which the DPA conducted the proceedings does not comply with Article 57 of the GDPR. However, since the complainants were unable to respond, the debates were reopened at the request of the Litigation Chamber.

A.8. - Hearing and reopening of debates

156. In accordance with Article 51 of the Rules of Procedure of the Data Protection Authority, a hearing was organised, to which all parties shall be invited. The hearing took place on 11 June 2021.
157. An official report of the hearing was drawn up in order to give details and additional information which were made during the hearing, without repeating the elements set out in the submission. The parties were also given the opportunity to submit their written comments on the record. A number of elements mentioned below are relevant to the present decision.
158. In the context of the hearing, the Inspection Service first confirmed its position that IAB Europe acts as a data controller for the processing of personal data under the Transparency and Consent Framework (hereinafter "TCF"), but not for OpenRTB.
159. The Inspection Service also clarified that personal data is collected as provided for in the *TCF Policies*, in the *Terms and Conditions*⁴² and in the privacy policy, as well as in the context of the TC String values stored in a *euconsent-v2* cookie, the latter as an expression of a user's preferences must also be regarded as personal data. The Inspection Service also emphasises that the TC String as such does not contain any information relating directly or indirectly to the taxonomy of the website to which the TC String refers. This last aspect concerns an essential distinction between the preferences of the user that are collected in the context of the TCF, and the personal data of that same user that are collected and distributed within the OpenRTB system. In conclusion, the Inspection Service states that the TC String values and the *euconsent-v2* cookie do not in themselves allow the identification of an individual user. Although both elements contain personal data, in the sense that the information relates to one natural person, the Inspection Service also confirms that it is not possible to identify the specific data subject on the basis of that information alone.
160. During the hearing, the defendant raised a procedural point, namely that the Litigation Chamber is not permitted to rule on the complainants' submission before an analysis has been carried out on the consistency of their written submissions in comparison with the complaints. The defendant also requests that the Litigation Chamber rule on the necessity of requesting a supplementary investigation by the Inspection Service, as allegedly required by Article 57.1.f GDPR. The Litigation Chamber will decide on this procedural point in the present decision⁴³.

⁴² Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33), p. 7.

⁴³ See para. 174 et seq. of this decision.

161. The complainants responded orally to the defendant's procedural arguments during the hearing.
162. With regard to the timing of the TC String generation, the defendant emphasises that the capture of the exact creation time cannot lead to the uniqueness of a TC String, as there is a chance that two unidentified users may give the same preferences at the same time. Moreover, this timestamp alone is not sufficient to speak of a unique string, since the values of the TC String are not persistent and may vary over time or according to the visited websites.
163. The defendant also states that the *global consent* cookies scenario, in which the preferences stored in one TC String apply across several websites, is not relevant in view of the limited scope at the time of the hearing⁴⁴, as well as the intention of IAB Europe, as a result of the finding that a global consent does not meet the requirement of a specific consent⁴⁵, to stop supporting this functionality and to phase it out in the weeks following the hearing.
164. As regards the question whether the allocation of a subdomain of *consensu.org* to CMP by means of a DNS delegation can be regarded as a determination of the means of processing, the defendant submits that, as a result of the DNS delegation, each subdomain refers to servers of the CMPs, which are moreover the only ones able to read the TC Strings from the users' devices. In addition, the defendant submits that the registration of a subdomain of *consensu.org* is purely optional and, as such, does not constitute an essential means of processing.
165. The complainants emphasise, on the other hand, that a DNS delegation can always be reversed by the defendant, and that it is irrelevant that the defendant does not have access to the *euconsent-v2* cookies. The complainants also point out that the DNS delegation can be regarded as an essential means of processing, since the DNS delegation is used to distribute the TC String further through the TCF ecosystem.
166. Concerning the existence of interfaces between the TCF and OpenRTB, the complainants stress that both systems are inherently intertwined because of the link between, on the one hand, the TC String that the CMPs generate according to the instructions of the TCF and, on the other hand, *bid requests*, which are regulated by the OpenRTB. In other words, the latter are used as vehicles to spread the TC String throughout the OpenRTB ecosystem.

⁴⁴ According to the defendant, the number of globally scoped consents was at most 0.5% of all consent and preferences collected worldwide.

⁴⁵ Article 4.11 GDPR: "consent" of the data subject means any freely given specific, informed and unambiguous expression of will by which the data subject accepts, by declaration or unambiguous active act, the processing of personal data relating to him or her.

167. The defendant states that both systems can function independently and that the TCF was developed with OpenRTB as a starting point and could be used in that context, as OpenRTB is the most widely used standard in the industry. According to the defendant, this does not mean that the TCF is an essential means of using OpenRTB.
168. The defendant argues that the elaboration by the defendant of a future Code of Conduct in relation to the TCF cannot be regarded as proof of its (shared) responsibility for the processing of personal data in the context of the TCF. Complainants add that it is impossible to verify compliance with the GDPR by participating organisations, even if the rules are clearly defined in an enforcement policy.
169. In this regard, the defendant refers to the development and gradual implementation of automated compliance programmes to monitor the extent to which CMPs and advertisers (as well as other *adtech vendors*) comply with the TCF Policies, including future internal audits of the processes at the aforementioned parties. The defendant also emphasises that the TCF already provides for sanctioning measures against *adtech vendors* that do not adhere to the framework, such as temporary suspensions of their participation in the TCF.
170. With regard to the link between the TC String and the individual user, the defendant takes the view that the TCF does not determine how this is done, nor how the TC String is subsequently communicated to the *adtech vendors*, as these elements are entirely subject to the OpenRTB specification.
171. The defendant clarifies that the use of the *consensu.org* domain is purely optional, and moreover, this domain was not developed for the purpose of processing or storing logs related to the TC Strings.
172. Finally, the defendant emphasises its position that the TC String only constitutes personal data after it has been linked in the context of the OpenRTB to a *bid request* which already contains personal data.
173. On 9 August 2021, after deliberation, the Litigation Chamber decides to reopen the debates on specific procedural arguments of IAB Europe.
174. On 23 August 2021, the Litigation Chamber received the first submissions from the defendant. The defendant states that the DPA infringed Article 57.1.a and 57.1.f GDPR and Article 94(3) DPA Act. The DPA also allegedly failed to comply with the principle of sound administration and the defendant's rights of defence.
175. With regard to Article 57.1.f GDPR, the defendant first of all claims that the complainants have submitted new allegations in their submission, which are thus more extensive than the original complaints. Moreover, according to the defendant, the DPA did not proactively investigate these new allegations by charging the Inspection Service with a new or

supplementary investigation. As a result, the defendant considers that the DPA has failed to fulfil its duties under Article 57.1.f GDPR.

176. Furthermore, the defendant claims that, by requesting an initial investigation from the Inspection Service, the Litigation Chamber has *de facto* bound itself to a procedure in which every allegation or defence must be investigated by the Inspection Service. According to the defendant, the decision of the Litigation Chamber not to request a supplementary investigation after an initial investigation and the submission of the defences led to an infringement of Article 94(3) DPA Act.
177. The defendant also states that, in the absence of an investigation by the Inspection Service into supposed new allegations in the complainants' defences and a legal classification of those allegations, it was unable to defend itself adequately against the complaints made against IAB Europe. Thus, the procedure before the Litigation Chamber could be considered to have evolved from an *inquisitorial* to an *adversarial* procedure in which the Litigation Chamber would no longer have acted as an administrative dispute resolution body, taking mainly into account the claims and documents of the complainants, with the result that the rights of defence of IAB Europe have been violated, according to the defendant.
178. On 6 September 2021, the Litigation Chamber received the complainants' submission. The complainants consider, first of all, that the defendant's new pleas exceeded the limited scope of the reopened debates.
179. Secondly, the complainants argue that the nature of the proceedings has not changed in any way, as the proceedings were started because of complaints made to the DPA, in other words, as an *adversarial* procedure, and have remained so throughout.
180. Thirdly, the complainants refer to Articles 63(2) and 94 DPA Act, as a counter-argument to the assertion that the Litigation Chamber should have had the Inspection Service examine each of the pleas raised by the complainants. After all, these provisions provide the Litigation Chamber with a discretionary power to decide whether or not an (additional) investigation by the Inspection Service is necessary.
181. Furthermore, the complainants argue that it is impossible for the Litigation Chamber to have an investigation or supplementary investigation carried out by the Inspection Service after the parties' submissions and exhibits, taking into account the time limit of 30 days after, respectively, the referral to the Litigation Chamber by the First Line Service following the lodging of the complaint, or the Litigation Chamber's reception of the Inspection Service's initial investigation report, under Article 96 of the DPA Law.
182. With regard to the defendant's argument that the way the Litigation Chamber handled the case violates Article 57.1.f GDPR, the complainants point out that, first of all, this provision has no direct effect in the sense that the defendant can derive rights from it. The complainants also argue that this provision cannot affect the internal structure and

functioning of the supervisory authorities, which, with regard to the DPA and, more specifically, the division of powers between its Inspection Service and its Litigation Chamber, are subject to Belgian administrative (procedural) law.

183. Furthermore, the complainants state that Article 57.1.f GDPR does not refer to an obligation on the part of the Litigation Chamber to request an investigation by the Inspection Service into the complaints, but to the power of the supervisory authorities to close the case.
184. In addition, the complainants argue that the decision of the Litigation Chamber to request an investigation from the Inspection Service in no way prevents it from relying on the submissions and exhibits submitted by the parties, contrary to the defendant's position.
185. As regards the defendant's alleged failure to comply with the principle of due care, the complainants submit that the Litigation Chamber is required under that principle to study properly all the exhibits in the file so that its decision is based on a correct and complete presentation of the facts. However, this principle again does not imply in any way that the Litigation Chamber must have a (supplementary) investigation carried out by the Inspection Service for every exhibit.
186. As regards the defendant's rights of defence, the complainants maintain that, on the basis of the Inspection Service's various investigative reports and the submissions and exhibits submitted by the complainants, the defendant was adequately informed of the alleged facts and infringements of law. Also, according to the complainants, the defendant was given sufficient opportunity to defend itself in writing against the legal and factual allegations made by the complainants, given that the defendant was offered two rounds of submissions.
187. Finally, the complainants refer to the lack of concrete examples, in the defendant's latest submissions, of alleged new allegations on which the defendant was unable to conclude or which were not investigated by the Inspection Service.
188. On 13 September 2021, the Litigation Chamber received the defendant's response.
189. According to the defendant, only the inspection report determines the extent of the allegations, provided that the inspection report is meaningful and based on a comprehensive examination of the facts. Furthermore, the defendant submits that the decision of the Litigation Chamber to request an investigation by the Inspection Service has resulted in the procedure as a whole becoming an "*inquisitorial*" procedure, irrespective of whether the procedure has its origin in the complaints filed with the DPA. According to the defendant, the decision of the Litigation Chamber not to subsequently request a supplementary investigation and to base the further proceedings solely on the parties' submissions and exhibits amounts to a breach of its rights of defence.

190. In addition, the defendant is of the opinion that the period of thirty days provided for in Article 96(1) DPA Act does not apply to the request by the Litigation Chamber to have a supplementary investigation carried out by the Inspection Service.
191. The defendant bases that reasoning on the distinction made in general administrative law between expiry periods and periods of order. In particular, the defendant takes the view that, in the absence of formal provisions in the DPA Act to the effect that exceeding the 30-day time limit results in a loss of jurisdiction for the Litigation Chamber, the time limits provided for in Article 96 must be complied with, although not on pain of invalidity of the decision rendered too late. According to the defendant, the Litigation Chamber therefore remains competent to make a decision for supplementary investigation even after the expiry of the 30-day period of order. That interpretation, the defendant argues, is in fact the result of the greater importance of the right to a defence over the right to expeditious proceedings before the Litigation Chamber.
192. As regards the direct effect of Article 57.1.f GDPR, the defendant submits that the existence of a margin of appreciation for the Member States does not exclude the direct effect of a provision, but implies an examination of whether that provision is intended to provide a guarantee for the parties. The defendant takes the view that Article 57.1.f GDPR fulfils this requirement and clarifies that its argument for requesting an supplementary investigation is furthermore limited to an assessment in fact and in law of the supporting points in the proceedings.
193. In conclusion, the defendant states that it has not received a clear statement of the nature and scope of the charges, except for the allegations made in the complainants' defences. In that regard, the defendant submits that the technical inspection reports contain merely technical descriptions, in which, moreover, the TC String is not mentioned anywhere. In Section A.9. - Procedural objections raised by the defendant, the Litigation Chamber will demonstrate why the procedural rights, including those relating to the specificity of the charges, were sufficiently respected.

A.9. - Procedural objections raised by the defendant

A.9.1. - Infringements of procedural rules applicable to the inspection report and of fundamental rights and freedoms of IAB Europe

a. Inadmissibility of the complaints

194. The defendant first of all argues that some of the complaints were filed in English and therefore do not meet the formal admissibility requirements set out in Article 60 DPA Act.

195. In addition, the defendant takes the view that some of those filing the complaints cannot be regarded either as "complainants" or as "parties" within the meaning of Articles 93, 95, 98 and 99 DPA Act, with the result that their submissions must be excluded from the debates and cannot be taken into account.
196. Finally, the defendant asserts that the measures that the DPA can impose under Article 100 of the DPA Act do not provide any benefit to these complainants.
197. IAB Europe thus considers that the case was unlawfully initiated - in particular on the basis of several inadmissible complaints - with the result that the claims against IAB Europe must be rejected and cannot lead to the imposition of a valid sanction or corrective measure on IAB Europe.

Position of the Litigation Chamber

198. The Litigation Chamber refers to Article 77.1 of the GDPR, according to which data subjects have the right to lodge a complaint in the Member State where they usually reside, have their place of work or where the alleged infringement was committed. The four complaints in English referred to by the defendant were not lodged directly with the DPA, but with the national supervisors with jurisdiction for each of the complainants, in accordance with the locally applicable language legislation. *In casu*, the four complaints have been filed respectively with the Polish supervisory authority, with the Slovenian SA, with the Italian SA as well as with the Spanish SA, which then referred these complaints to the Belgian DPA as the lead supervisory authority, in accordance with the cooperation procedure provided for under Article 56 GDPR.
199. The formal admissibility requirements provided for under Article 58 DPA Act, and more specifically the requirement that a complaint be drawn up in one of the national languages, only apply to complaints filed directly with the DPA. Any other view would erode the effective operation of the right to complain, one of the core elements of the GDPR. Indeed, a complainant who submits his complaint to an authority of a Member State cannot be expected to submit it in the language of the Member State of the lead authority, if that is different from the authority to which he submits his complaint. It follows that the four complaints in question were validly filed with the DPA.
200. In relation to the lack of interest of *Fundacja Panoptikon*, as well as other complainants, in the complaints lodged through the European "one-stop shop" mechanism, raised by the defendant, the Litigation Chamber notes that *Fundacja Panoptikon* lodged the complaint with the Polish supervisory authority on behalf of Ms Katarzyna Szymielewicz in accordance with Article 80.1 GDPR. On the basis of this provision, the complainant has the right to instruct *Fundacja Panoptikon* to lodge the complaint on its behalf.

201. The Litigation Chamber notes that IAB Europe does not explain at all why *Fundacja Panoptikon* should not be considered a complainant and party here. In addition, in the absence of doubts whether the other complaints were admissible, the argument by the defendant would not make any difference towards the outcome of this decision.

202. This argument must therefore be rejected.

b. The inspection report is not properly reasoned

203. The defendant then goes on to address the inadequate reasoning in the inspection report. As a result of the lack of a clearly worded statement of reasons in the inspection report - including the lack of a clearly identified data controller in connection with a clearly defined data processing activity - the defendant argues that the inspection report not only infringes the DPA's obligation to provide express and sufficient reasons for its decisions, but also constitutes a clear breach of IAB Europe's rights of defence. Consequently, the inspection report infringes IAB's rights of defence as laid down in Article 6 ECHR and Article 47 of the Charter of Fundamental Rights.

Position of the Litigation Chamber

204. IAB Europe's claim that the Inspection Service's report of 13 July 2020 is not sufficiently reasoned is incorrect. As can also be seen from the reflection of this Inspection Report in this decision, the Inspection Report contains detailed reasoning.

205. Furthermore, IAB Europe overlooks the fact that, in addition to the report of 13 July 2020, the Inspection Service produced other very extensive and detailed technical reports (Exhibits 24 and 53). Finally, the Litigation Chamber points to the extensive written and oral exchange of views between the parties before its Chamber. IAB Europe's simple assertion of failure to respect its rights of defence is therefore without merit, as set out in the following paragraphs.

c. Incompleteness and bias of the inspection report

206. The defendant refers to Article 58.4 GDPR, which provides that the procedure before the DPA must be conducted in compliance with "*appropriate safeguards, including [...] the due process of law*". According to the defendant, that principle applies equally to the investigation carried out by the Inspection Service and to the findings set out in the inspection report.

207. Referring to the similarities with the role and duties of a prosecutor in ordinary criminal proceedings, the defendant claims that the basic principles of loyalty, impartiality and independence also apply to the Inspection Service. The defendant refers to Section IV of its submission and considers that relevant exculpatory elements, of which the Inspection Service was or should have been aware, are missing from the inspection report.

208. The defendant, emphasising that the DPA is obliged to maintain the presumption of innocence of a defendant at all times, including during the investigative phase of proceedings which may lead to penalties of a criminal nature within the meaning of Article 6 ECHR, considers that its presumption of innocence has been infringed and that the claims against IAB Europe must therefore be dismissed.

Position of the Litigation Chamber

As regards the autonomy of the Litigation Chamber from the other bodies of the DPA, including the Inspection Service

209. The Litigation Chamber first notes that the defendant seems to confuse the role and prerogatives of the Litigation Chamber with those of the other bodies of the DPA.
210. As indicated above, the Litigation Chamber is the administrative disputes body of the DPA pursuant to Article 33(1) DPA Act. The provisions governing the procedure before the Litigation Chamber (see Articles 92 to 100 DPA Act) do not show that it is in any way bound by the findings of any other body of the DPA. Consequently, the Litigation Chamber is not bound by the findings of the Inspection Service.
211. It is also recalled that the Inspection Service submitted not one but several detailed and technical reports clearly setting out the deficiencies attributable to the defendant and substantiating its position with the help of legislative, jurisprudential and factual sources, as the complainants point out. The defendant had access to those reports. Moreover, the defendant responded in detail to the reports of the Inspection Service.
212. The defendant further submits that the Inspection Service's report of 13 July 2020 is not exculpatory, but merely incriminating, because the report does not contain "certain exculpatory elements" of IAB Europe. The defendant also refers, without further specification, to Section IV of its submission, in which it sets out its arguments on the merits. In the absence of more detailed information on the exculpatory elements that were omitted from the abovementioned report of the Inspection Service, that complaint must be rejected.
213. The Litigation Chamber notes that even if the defendant's argument were to be followed, *quod non*, it could nevertheless be concluded, as the Market Court has already indicated, that the proceedings before the Litigation Chamber were not unlawful in so far as both parties were given the opportunity to put forward their arguments in their submissions⁴⁶. In view of the complexity of the system, the Litigation Chamber was not able to specify every technical aspect of the system against which charges were brought against the defendant

⁴⁶ Market Court, 2019/AR/741, 12 June 2019, p. 12, available on the website of the DPA.

at the outset of the proceedings before the Litigation Chamber, on 13 October 2020, i.e. at the time when the parties were invited to present their written submissions (art. 98 DPA Act). However, in order to ensure the procedural rights of the parties, the Litigation Chamber firstly ensured that the defendant had sufficient opportunities to present its arguments before the Litigation Chamber, and secondly, that it remained within the scope of the initial complaints and the Inspection Services' reports, communicated to both parties prior to their written submissions.

As regards the legal framework for the Inspection Service's investigations

214. It should also be recalled that the Inspection Service may conduct any investigation, hold any hearing and collect any information it deems useful in the course of its duties in order to ensure compliance with the fundamental principles of personal data protection⁴⁷.
215. The Litigation Chamber also points out that the intervention of the Inspection Service in the proceedings consists of recording findings and that it has no power to impose penalties.
216. Contrary to the defendant's contention, the Inspection Service is not an administrative authority of criminal law within the meaning of Article 6 of the European Convention on Human Rights (hereinafter: "ECHR"), as it has no power to impose penalties and its task is limited to making findings and transmitting them to the Litigation Chamber in its report. As indicated above⁴⁸, the findings of the Inspection Service are only elements on which the Litigation Chamber bases its decision at a later stage of the proceedings. Nevertheless, the Litigation Chamber emphasises that the Inspection Service's investigation in the present case was conducted in an impartial manner, in accordance with the requirements of Article 6 ECHR and Article 47 Charter. It disagrees with suggestions made by the defendant in so far as they call into question the impartiality of the Inspection Service.

On respect for the right to a fair trial, including the right to a defence before the Litigation Chamber

217. The Litigation Chamber agrees with the defendant on the importance of applying procedural safeguards relating to due process in the disputes before it. It is also established that these principles are effectively applied before the Litigation Chamber.

⁴⁷ Cf. Art. 64 DPA Act: "The Inspector General and the inspectors shall exercise the powers referred to in this Chapter for the purpose of supervision as provided for in Article 4(1) of this Act". Also see Art. 72(1) DPA Act: "Without prejudice to the provisions of this Chapter, the Inspector General and the inspectors may conduct any enquiry, control or audit, as well as collect any information they consider useful in order to ensure that the fundamental principles of the protection of personal data, within the framework of this Act and the laws containing provisions relating to the protection of processing of personal data, are effectively respected" (emphasis added).

⁴⁸ See para. 209-210 of this decision.

218. As set out above⁴⁹, the defendant's complaint concerning the alleged lack of reasoning and impartiality of the Inspection Service's report, on which the defendant relies to conclude that its right to a fair trial has been violated, must be rejected.
219. For the sake of completeness, the Litigation Chamber also points out that the Market Court has already ruled that — in the event that the procedural safeguards in the earlier stage of the proceedings were not guaranteed, *quod non* — parties have an adequate remedy against decisions of administrative bodies, in particular through the possibility of appeal to the Market Court⁵⁰.
220. The Market Court added that a lack of impartiality on the part of an administrative authority does not necessarily constitute an infringement of Article 6.1 ECHR if a judicial authority with full power of review, which itself respects the guarantees of Article 6.1 ECHR, can review the decision at issue.
221. According to the Market Court, an infringement of the principle of impartiality of the administration at an earlier stage does not necessarily entail a breach of the right to a fair trial if that infringement can be remedied at a subsequent stage. The possibility of an appeal to a court that respects the guarantees of Article 6 ECHR is intended to allow precisely such corrections⁵¹.
222. Specifically with regard to the Litigation Chamber, the Market Court ruled as follows:
- "[...] even then, this legal protection by the legal subject is only legally enforceable before a judge (who is part of the judiciary) [...]. The legal possibility of bringing an action/recourse before the Market Court is intended to provide the litigant with the guarantee of Article 6.1 ECHR and, more particularly, with the remedy provided for in Article 47 CFREU [Charter of Fundamental Rights of the European Union]"*⁵²
223. Therefore, in the absence of impartiality on the part of the Litigation Chamber, which is not the case here, and in so far as the Market Court exercises full judicial review of the decisions of the Litigation Chamber, it cannot be concluded, *ipso facto*, that the right to a fair hearing in the proceedings has been infringed.
-

⁴⁹ See para. 204 et seq. of this decision.

⁵⁰ "The legislator has given the citizen a conclusive legal remedy against the conduct of administrative bodies (in this case the DPA) by providing precisely recourse to the Market Court", Court of Appeal Brussels, Market Court section, 19th Chamber A, Market Court section, 2019/AR/741, 12 June 2019, p. 9. The judgements of the Market Court are available on the website of the DPA in their original language (Dutch or French).

⁵¹ "A lack of objective or structural impartiality on the part of an administrative authority does not necessarily constitute an infringement of Article 6.1 ECHR if the decision of that authority can subsequently be reviewed by a court of law with full jurisdiction and which offers all the guarantees provided for in Article 6.1. Consequently, an infringement of the principle of impartiality at an earlier stage does not necessarily lead to a denial of the right to a fair trial if that infringement can still be rectified at a later stage. The organisation of an appeal to a body that meets all the safeguards of Article 6 ECHR serves to make such redress possible", Court of Appeal of Brussels, Market Court Section, 19th Chamber A, Market Cases Chamber, 2019/AR/741, 12 June 2019, p. 10.

⁵² Court of Appeal of Brussels, Market Court Section, 2020/AR/329, 2 September 2020.

224. For the sake of clarity and information, the Litigation Chamber notes that while the right to a defence forms part of the fundamental rights that constitute the legal order of the Union and are enshrined in the Charter⁵³, the fact remains that, as the CJEU has held, the various components of the right to a fair trial, including the right to a defence, are not absolute in nature and that any restriction may be possible for a public interest purpose. This assessment must be made *in concreto*:

“However, the Court has already ruled that fundamental rights, including respect for the right to a defence, are not absolute but may include restrictions, provided that they genuinely meet the objectives of general interest pursued by the measure in question and that, having regard to the objective pursued, they cannot be regarded as constituting a disproportionate and intolerable interference impairing the very substance of the rights guaranteed [...].”

34. Moreover, whether the right to a defence have been infringed must be assessed in the light of the specific circumstances of each case [...]”⁵⁴.

A.9.2. - Infringements of the fundamental rights and freedoms of IAB Europe with regard to the general nature of the procedure for the DPA

a. Administrative penalties and Articles 6 and 7 ECHR and Article 47 of the Charter of Fundamental Rights of the European Union

225. The defendant submits that the measures and fines which the DPA is authorised to impose in the context of Articles 100 and 101 DPA Act, read in conjunction with Article 83 GDPR, must be classified as penalties of a criminal nature within the meaning of international human rights conventions such as the ECHR and the Charter of Fundamental Rights, having regard to the very nature of the offences and the nature and severity of the penalties which may be imposed on a party. As a result, according to the defendant, Articles 6 and 7 ECHR and Article 47 Charter of Fundamental Rights are applicable to the penalties which the DPA may impose on IAB Europe.

226. The defendant then considers that the wide margin between the minimum and maximum amount of administrative penalties of a criminal nature, which, moreover, according to the defendant, puts all infringements on an equal footing while failing to specify the severity of the penalties in the law itself, is contrary to the fundamental principles of substantive legality and proportionality. The same reasoning applies to Articles 100 and 101 DPA Act, *in conjunction with Article 83 GDPR*, which, due to their imprecise and ambiguous wording, do

⁵³ In this regard, see CJUE, 18 July 2013, *Commission and Others v Kadi*, C- 584/10 P, C- 593/10 P and C- 595/10 P, ECLI:EU:C:2013:518, points 98 and 99.

⁵⁴ CJEU, 10 September 2013, C-383/13 PPU, *Affaire G. et R.*, ECLI:EU:C:2013:533, points 33 s.

not allow a party to appropriately assess the criminal law consequences of a certain conduct prior to its occurrence.

227. It would therefore follow that Articles 100 and 101 DPA Act, in conjunction with Article 83 GDPR, are contrary to the fundamental principles of substantive legality and proportionality laid down in Articles 6 and 7 of the ECHR and Article 47 of the Charter of Fundamental Rights. For those reasons, the defendant considers that Articles 100 and 101 DPA Act, read in conjunction with Article 83 GDPR, cannot constitute a valid legal basis for the DPA to impose a sanction on IAB Europe.

Position of the Litigation Chamber

228. First of all, the power to impose an administrative fine and the modalities of its application are laid down in the directly effective Article 83 of the GDPR. In line with the case law of the Market Court, the Litigation Chamber finds that administrative fines, together with the other corrective measures provided for in Article 58 GDPR, form a powerful part of the enforcement tools available to the DPA⁵⁵.
229. If the DPA finds one or more infringements of the regulations, it must determine the most appropriate corrective measure(s) to address that infringement. The measures available for this purpose are listed in Article 58.2.b to 58.2.j GDPR. In particular, Article 58.2.i GDPR provides that the supervisory authority has the power, depending on the circumstances of each case, to impose, in addition or instead of the measures referred to in this paragraph, an administrative fine pursuant to Article 83 GDPR. This means that an administrative fine can be both a stand-alone (corrective) measure and a measure taken in conjunction with other corrective measures (and is therefore a kind of complementary measure). The criminal provisions of Sections 83.4 to 83.6 GDPR allow the imposition of an administrative fine for most infringements. Nevertheless, the supervisory authority has the responsibility to always choose the most appropriate measure(s)⁵⁶.
230. In addition to the relevant provisions of the GDPR and the DPA Act on the level of administrative fines that the Litigation Chamber may impose, the Litigation Chamber also relies on the case law of the Market Court⁵⁷, which formulates requirements on the predictability and reasoning of administrative fines imposed by the Litigation Chamber. For example, this case law has resulted in a form notifying the intention to impose a sanction being submitted to the party concerned, who may react to it and send its comments to the

⁵⁵ Court of Appeal Brussels, Market Court Section, 2021/AR/320, 7 July 2021, p. 38.

⁵⁶ *Ibidem*.

⁵⁷ Among others, judgments of 19 February 2020 (2019/AR/1600), of 24 January 2021 (2020/AR/1333) and of 7 July 2021 (2021/AR/320).

Litigation Chamber before it takes a decision. Accordingly, in the present procedure, this form was sent and the defendant submitted a reaction⁵⁸.

231. The Litigation Chamber also refers to the case law of the Market Court, which determined that the GDPR does not provide for a specific fine tag or range for specific infringements, but only an upper limit or maximum amount. In practice, this means that the DPA can decide not only not to impose a fine on the offender, but also that, if it decides to impose a fine, it shall be between the minimum, starting at 1 EUR, and the maximum foreseen. The fine shall be decided by the DPA taking into account the criteria listed in Article 83(2) GDPR⁵⁹.
232. Furthermore, the Litigation Chamber also follows the Article 29 Data Protection Working Party's guidelines on the application and setting of administrative fines under the GDPR, endorsed by the EDPB⁶⁰, which detail the criteria of Article 83(2) GDPR that a supervisory authority must apply when assessing whether to impose a fine, as well as the amount of the fine.
233. Furthermore, these guidelines also contain an explanation of Article 58 GDPR relating to the measures that a supervisory authority may choose to take, as the remedies are inherently different in nature and essentially have different purposes. Finally, it specifies that certain measures under Article 58 GDPR may be cumulative and thus constitute a regulatory action based on several remedies.
234. The Market Court, ruling with full jurisdiction, performs a legality and proportionality test of the sanction and will (only) reduce or cancel the fine in case of serious and proven circumstances that the Litigation Chamber would not or not sufficiently take into account.
235. In short, this system sufficiently guarantees that the fundamental legal principles arising from Article 6 of the ECHR and Article 47 of the Charter are complied with.

Legal framework for administrative fines

Relevant provisions in the DPA Act

236. Pursuant to Article 100(1)(13) of the DPA Act, the Litigation Chamber has the power to impose administrative fines. The Litigation Chamber may decide to impose an administrative fine on the prosecuted parties in accordance with the general terms and conditions set out in Article 83 GDPR.
237. Pursuant to Article 103 DPA Act, if an offender has committed several infringements by means of the same act only the heaviest administrative fine of the respective infringements

⁵⁸ See para. 272-273.

⁵⁹ Court of Appeal Brussels, Market Court Section, 2021/AR/320, 7 July 2021, p. 42.

⁶⁰ EDPB - Guidelines on the application and setting of administrative fines for the purposes of Regulation (EU) 2016/679, WP253, published on <http://www.edpb.europa.eu>.

shall apply. In the event of overlapping infringements, the rates of the administrative fines shall be added together without the total amount exceeding twice the highest amount of the fine applicable to the infringements committed.

Relevant provisions in the GDPR

238. Once an infringement of the Regulation has been established, based on the assessment of the facts of the case, the competent supervisory authority should determine the most appropriate corrective measures to address the infringement. The provisions of Article 58(2)(b)-(j)⁶¹ set out the tools that supervisory authorities can use to address non-compliance by a data controller or processor.
- a. to issue warnings to a data controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
 - b. to issue reprimands to a data controller or a processor where processing operations have infringed provisions of this Regulation;
 - c. to order the data controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
 - d. to order the data controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
 - e. to order the data controller to communicate a personal data breach to the data subject;
 - f. to impose a temporary or definitive limitation including a ban on processing;
 - g. to order the rectification or erasure of personal data or the restriction of processing pursuant to Articles 16, 17 and 18 GDPR, as well as the notification of such actions to recipients to whom the personal data have been disclosed, in accordance with Articles 17(2) and 19 GDPR;
 - h. to revoke a certification, or order the certification body to revoke a certification issued under Articles 42 and 43 GDPR, or order the certification body not to issue a certification if the certification requirements are no longer fulfilled;
 - i. depending on the circumstances of each case, in addition to or instead of the measures referred to in this paragraph, to impose an administrative fine pursuant to Article 83 GDPR; and;

⁶¹ Article 58(2)(a) states that a warning may be issued. In other words, in the case to which the provision relates, **there is not yet a breach of the regulation.**

- j. to order the suspension of data flows to a recipient in a third country or to an international organisation.

239. The power to impose an administrative fine is regulated in Article 83 GDPR, which reads as follows:

"General conditions for the imposition of administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
- b) the intentional or negligent character of the infringement;*
- c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
- d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
- e) any relevant previous infringements by the controller or processor;*
- f) the categories of personal data affected by the infringement;*
- g) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
- h) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*
- i) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*
- j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- b) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;*
- c) the obligations of the certification body pursuant to Articles 42 and 43;*
- d) the obligations of the monitoring body pursuant to Article 41(4).*

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- b) the data subjects' rights pursuant to Articles 12 to 22;
- c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- d) any obligations pursuant to Member State law adopted under Chapter IX;
- e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. [...]”

240. A reading of points (a) to (k) of Article 83(2) GDPR, as well as the additional explanations in paragraphs 3 to 6 of that same provision, is sufficient to refute the defendant's argument that the various offences listed in Article 83 RGPD are placed on an equal footing.
241. The various criteria to assess the severity of the penalties are clearly set out in Article 83 itself and in recitals 148 to 150 GDPR. Article 83.2 also makes it clear that an analysis must be made "according to the circumstances of the case".
242. The Litigation Chamber already referred to the Guidelines on the application and setting of administrative fines under the GDPR, endorsed by the EDPB. These Guidelines provide guidance on the interpretation of the individual facts of the case in the light of the criteria set out in Article 83.2 GDPR. The Guidelines bind the Litigation Chamber as an organ of the DPA, a member of the EDPB.
243. In order to strengthen the enforcement of the rules of the GDPR, recital 148 GDPR clarifies that penalties, including administrative fines, should be imposed for any breach of the Regulation, in addition to or as an alternative to appropriate measures imposed by the supervisory authorities under this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the data controller or

processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

244. Contrary to what the defendant maintains, the GDPR does not therefore impose a minimum amount of fine, but only maximum amounts which, depending on the infringements committed, may amount to 2% or 4% of the turnover of a data controller, or EUR 10,000,000 or 20,000,000 respectively. These amounts are of a dissuasive nature, and it is for the Litigation Chamber to modulate the amount of the fine according to the circumstances of the case, taking into account the requirement of proportionality and with a view to ensuring the effectiveness of the provisions of the GDPR.
245. Since the various offences listed in Article 83 GDPR are not treated in the same way and since the various criteria to assess the severity of the penalties are clearly set out, the defendant's argument that the combined reading of Article 83 GDPR and Articles 100 and 101 DPA Act infringes the principles of legality and proportionality, and thus Articles 6 and 7 ECHR and 47 of the Charter of Fundamental Rights of the European Union, because of its vagueness must be rejected.
246. Article 83 GDPR is a directly effective provision of an EU Regulation and it is the task of the Litigation Chamber to ensure the effective operation of this Regulation. It is not for the Litigation Chamber, as a body of a national administrative authority, to rule on the possible unlawfulness of that provision.
247. In addition, the Constitutional Court ruled in its judgment no. 25/2016, of 18 February 2016 (p24-28) that a single, wide margin for an administrative fine, allowing the administrative authority to adjust the administrative fine to the gravity of the infringement, does not violate the principle of legality:

"B.18.2. [...] The principle of legality in criminal matters, which derives from the aforementioned constitutional and treaty provisions, is also based on the idea that the criminal law must be formulated in terms which enable any person, at the time when he adopts a course of conduct, to determine whether that conduct is punishable or not and, where appropriate, to know the sanction to be imposed. [...]

However, the principle of legality in criminal matters does not prevent the law from granting the court discretion. Indeed, the general nature of the laws, the diverse situations to which they apply and the evolution of the conduct they punish must be taken into account.

B.18.3. In the same way, to determine whether the ranges between the upper and lower limits of the sentences considered by the ordering body are so broad as to infringe the principle of the foreseeability of the sanction, account must be taken of the specific features of the offences to which those penalties are attached. [...]

B.20.1. The assessment of the seriousness of a crime and of the severity with which the crime may be punished is within the discretion of the competent legislature. It may impose particularly severe penalties in cases where the offences may seriously affect the fundamental rights of individuals and the interests of the community. It is therefore up to the competent legislator to establish the limits and amounts within which the discretion of the court and of the administration must be exercised. The Court could only reject such a system if it were manifestly unreasonable.

B.20.2. The ordering body cannot be blamed for wanting to rationalise and simplify the environmental criminal law in force in the Region. In order to achieve that objective, it could establish a single and sufficiently wide margin between the upper and lower limits of the sanction, both for criminal penalties and for alternative administrative fines, in order to allow the court or the administrative authority to adjust the sanction or the alternative administrative fine to the seriousness of the crime.

B.20.3. With regard specifically to the offence of exceeding the noise standards laid down by the Government, the contested provisions are addressed to persons subject to the law who are professionals and can assess with sufficient accuracy the seriousness of the offence they are committing and the corresponding severity of the sanction to which they are subject. In addition, the choice of sanction must be justified, either by the judge or by the administrative authority. In the latter case, the decision is subject to judicial review.

B.20.4. It follows from the foregoing that the contested provisions do not confer on the court or administrative authority any discretion going beyond the limits of what is permissible under the principle of the foreseeability of penalties

248. The defendant's argument that Articles 100 and 101 DPA Act in conjunction with Article 83 GDPR, which form the basis of the power of the Litigation Chamber to impose administrative penalties and fines, infringe the principles of legality and proportionality and thus the right to a fair hearing must therefore be rejected.

b. The internal rules of the DPA do not comply with the fundamental principle of the formal legality of criminal sanctions, enshrined in Articles 12 and 14 of the Belgian Constitution

249. The principle of formal legality, enshrined in Articles 12 and 14 of the Belgian Constitution, requires that the essential elements of the rules relating to the offences made punishable, the nature and level of the sanction, and the procedure guaranteeing that the right to a defence are safeguarded, be laid down by the Chamber of Representatives in accordance with the legislative procedure laid down by the Belgian Constitution.

250. Since this principle applies not only to criminal penalties *stricto sensu*, but also to administrative penalties of a criminal nature, it is fully applicable to the DPA sanctioning procedure.

251. In this regard, the defendant submits that various aspects of the DPA sanctioning procedure are not laid down in a legislative text - in particular, not in the DPA Act, but in the Rules of Internal Procedure of 15 January 2019 (RIO).
252. As a result, the defendant considers that the current proceedings were conducted on the basis of procedural rules that are contrary to Articles 12 and 14 of the Belgian Constitution and therefore lack a valid legal basis, with the result that the complaints against IAB Europe must be dismissed.

Position of the Litigation Chamber

253. The principle of legality means that the essential elements of an offence, such as its nature, the level of punishment and the procedural guarantees relating to it, must be determined by the legislator.
254. The Litigation Chamber notes that the only elements relating to the imposition of a sanction that are not contained in the GDPR, the DPA Act or the law of 30 July 2018, but in the Rules of Internal Order (RIO) of the DPA referred to by the defendant, are by no means essential elements for the imposition of fines. Indeed, it is not the nature of the fine, nor the sanction, that is at issue, but elements of a secondary or organisational nature, for example, with regard to the procedure to be followed in the absence of the president of the Litigation Chamber (Article 44 RIO), or the number of members sitting per case (Article 43 RIO).
255. The Litigation Chamber also emphasises that the independence of a supervisory authority under Article 51 et seq. GDPR means that the organisation of its processes, including for example the assignment of members to a procedure, is at the discretion of the Data Protection Authority, of course within the limits of the general principles of good administration and the relevant national legislation.
256. The defendant's argument that the procedure before the Litigation Chamber infringes the principle of legality is therefore rejected.

c. Appointment of members of the DPA violates Article 53 GDPR

257. The defendant claims that Article 39 DPA Act, which regulates the appointment of the members of the Litigation Chamber, does not in any way clarify the modalities of the appointment procedure. In particular, nowhere does it specify how the hearing of the candidates should proceed, nor does the DPA Act require a written record of the hearing. Moreover, the nomination takes place on the basis of a secret ballot and there are no guarantees as to the adequacy of the information on the candidates provided to the members of the Chamber of Representatives.
258. According to the defendant, the appointment of the members of the DPA, including the members of the Litigation Chamber, therefore does not satisfy the requirements of Article

53 GDPR, which provides that the appointment must be made 'by means of a transparent procedure'.

259. In view of the foregoing, the defendant considers that the members of the Litigation Chamber are not in a position to make a legally valid decision in relation to IAB Europe in this case. For those reasons also, the claims against IAB Europe should be dismissed.

Position of the Litigation Chamber

260. First of all, the Litigation Chamber points out that any imperfections in the appointment procedure of the members of the DPA cannot form part of these proceedings and that the parties cannot invoke a procedural interest in questioning the appointment procedure.
261. The Litigation Chamber reminds that the members of the Litigation Chamber are appointed by the House of Representatives and can only be removed from their positions by the House. Thus, neither the Litigation Chamber nor the Market Court are competent to rule on their appointment. In addition, the parties have no interests in requesting such a ruling.
262. Consequently, the Litigation Chamber rules that this plea is unfounded.

d. The way in which the DPA has handled this procedure is not in line with its duties and powers under Article 57 GDPR

263. In conclusion, the defendant states, both in its initial submission and in the context of the reopening of the debates, that the way in which the DPA, in addition to the original complaint, also considers the additional complaints and grievances made by the complainants, without the relevance of those additional allegations having been examined by the Inspection Service, makes the defence of IAB Europe considerably more difficult.
264. IAB Europe considers that this approach is not only fundamentally incompatible with the duties and responsibilities of a supervisory authority as defined in Article 57 GDPR, but also has the effect that IAB Europe must only defend itself against the allegations contained in the inspection report, as opposed to the subsequent allegations made by the complainants in their subsequent submissions.

Position of the Litigation Chamber

265. The Litigation Chamber emphasises first of all that at no time did the defendant explain which new allegations are the subject of their defences and as such would violate its rights of defence. For this reason alone, the Litigation Chamber considers itself entitled to declare the defendant's plea unfounded.
266. Secondly, the Litigation Chamber notes that the DPA Act in no way prescribes that the Litigation Chamber is bound by an investigation report following an investigation requested to the Inspection Service. Indeed, it does not follow from any provision of the DPA Act that the Litigation Chamber is denied the opportunity to take into account additional or

supplementary elements to the report of the Inspection Service, as long as the consideration of these additional or supplementary elements is sufficiently justified in the decision and the right of defence is sufficiently guaranteed.

267. The Inspection Service may in any case decide not to investigate certain disputed points, in accordance with its prerogative under Article 64(2) DPA Act. In such a case, however, it would be contrary to Article 57 GDPR as well as to the autonomy and independence of the Litigation Chamber, as implemented by Articles 92 to 100 DPA Act, to simply bind the Litigation Chamber to the findings of the Inspection Service, without taking into account the elements put forward in the debates by the parties in the course of the proceedings and in accordance with the right to be heard.
268. Thirdly, the Litigation Chamber rules that the alleged obligation to base debates on the inspection report alone following an investigation by the Inspection Service does not apply. The DPA Act does not provide anywhere that the Litigation Chamber should base its decision solely on the inspection report or on the parties' submissions. It is appropriate for a supervisory authority to also consult other bodies and sources in order to be able to support its decisions if necessary.
269. With regard to the Inspection Service's assessment with a view to a supplementary investigation, and in particular the nature of the time limits provided for in Article 96 DPA Act, the Litigation Chamber is not convinced by the arguments put forward by the defendant. In the present case, the parties have had ample opportunity to make their views known to the Litigation Chamber and to the other party regarding the allegations and charges, including the operation of the TCF, the processing of user preferences and permissions in the TC String, as well as the interrelationship between the TCF and OpenRTB.
270. In addition, the Litigation Chamber finds that there is no doubt about the crucial importance of the TC String for the functioning of the TCF. As a result, the defendant could have expected from the start of the proceedings that the debates would focus on the processing of data in the context of the TC String. Thus, there can be no question at all of new allegations - in so far as they exist, given the lack of any concrete example with which the defendant substantiated its plea - in the complainants' submissions, since they constitute an explanation of the operation of the TCF, which is not disputed as being at the heart of the complaints against IAB Europe.
271. Bearing the above points in mind, the Litigation Chamber rules that this plea is insufficient both in fact and in law.

A.10. - Sanction form, European cooperation procedure and publication of the decision

272. The procedure before the Litigation Chamber includes an exchange of written submissions as well as an oral hearing of the parties involved, as normal steps towards a decision. If the Litigation Chamber proposes, after deliberation, to impose a (punitive) sanction, the Market Court requires the Litigation Chamber to provide the defendant with an opportunity to respond to the intended sanctions, through a standard form covering the retained infringements and the criteria for determining the amount of the fine. This opportunity for contradiction, or right to be heard, pertains to the proposed sanctions only and is therefore only communicated to the defendant.
273. A sanction form has been sent on 11 October 2021, informing the defendant of its infringements against the GDPR as well as of the Litigation Chamber's intent to impose corrective measures and an administrative fine. IAB Europe submitted its response on 1 November, 2021. The defendant contests the calculation of the administrative fine, by claiming that the Litigation Chamber did not consider all relevant elements for determining the amount of the administrative fine under Article 83.2 GDPR. Moreover, the defendant disagrees with the Litigation Chamber's consideration of the total worldwide annual turnover of Interactive Advertising Bureau Inc. (IAB Inc.) for the calculation of the administrative fine, since the latter has no ownership stake in the defendant nor any say in the deployment of IAB Europe's activities. The defendant clarifies that IAB Europe licences the 'IAB' brand name from IAB Inc., and that the various IAB organizations across Europe are separate and distinct organisations.
274. On 8 November, the complainants submitted a request to the Litigation Chamber, asking to be provided with a copy of the sanction form as well as the defendant's reaction, based on the erroneous assumption that the defendant also received further insights into the draft decision of the Litigation Chamber. The Litigation Chamber responds on 9 November 2021 that it will not disclose the sanction form to the complainants. The notification of the sanction form to the defendant takes place within the framework of an objective review of legality and with the specific aim of respecting the defendant's rights of defence, in accordance with the case law of the Market Court. The defendant is thus informed in advance of the nature and severity of the sanction it risks and is given the opportunity to submit its final comments on this point to the Litigation Chamber. Notifying the sanction form to the complainants could not possibly contribute to the same objective, since the sanction envisaged would only be imposed on the defendant, not on the complainants, and would therefore not directly affect the interests of the latter. Neither the rights of the defence nor any other rule of law require that the complainants be able to put forward additional arguments in relation to the penalty which may be imposed on the defendant.

275. On 23 November 2021, the Litigation Chamber submitted its draft decision with the other concerned European supervisory authorities (hereinafter, ‘CSAs’), as foreseen under article 60.3 GDPR.
276. On 18 December 2021 the Litigation Chamber received a letter from the complainants in response to the Litigation Chamber’s decision not to disclose the content of the sanction form to the complainants. More specifically, the complainants argued that they should be informed whether the defendant has brought new elements to the proceedings. The Litigation Chamber notes that the debates were already closed at that time, and that the reaction of the defendant to the sanction form only pertained to elements concerning the sanction.
277. On 20 December 2021, the Litigation Chamber is notified through the Internal Market Information (IMI) system of a relevant and reasonable objection (RRO) submitted by the Dutch Authority for Personal Data (Autoriteit Persoonsgegevens). The objection pertains to the absence of reasoning by the Litigation Chamber with respect to the Dutch NGO Bits of Freedom’s claim that the TCF makes it impossible for users to exercise their data subject rights. The Litigation Chamber has addressed this RRO in its revised draft decision⁶².
278. On 21 December 2021, the defendant submitted a letter to the Litigation Chamber, requesting the suspension of the provisional enforcement of the decision, that the Belgian Data Protection Authority does not make the decision public until all appeals have been exhausted, and that the DPA refrains from issuing any public communication about the decision prior to any such final decision. Once again, the Litigation Chamber notes that the debates were already closed at that time.
279. On 21 December 2021, the Litigation Chamber is notified of a relevant and reasonable objection introduced by the Portuguese National Commission for Data Protection (CNPD). The objection pertains to the absence of sanction by the Litigation Chamber with respect to the processing of TC Strings in the absence of a lawful ground under Article 6 GDPR. The CNPD finds that the draft decision must impose upon the defendant the immediate erasure of all personal data unlawfully collected so far. The Litigation Chamber has addressed this RRO in its revised draft decision⁶³.
280. In addition to the two RROs, the Litigation Chamber received comments from other CSAs regarding the joint-controllership established by the Litigation Chamber, the use of legitimate interest for certain processing operations, the scope of the corrective measures,

⁶² See para. 504 to 506.

⁶³ See para. 535.

as well as the administrative fine envisaged and the relationship between IAB Inc. and IAB Europe.

281. On 13 January 2022, the Litigation Chamber submitted its revised draft decision with the other concerned European supervisory authorities (hereinafter, ‘CSAs’), as foreseen under article 60.5 GDPR.
282. On 17 January 2022, the Litigation Chamber notified the parties of the submission of the revised draft decision and the deadline of 27 January 2022 for the CSAs. It also clarified that the written exchanges with the defendant’s councils, concerning the sanction form, did not involve new arguments that would require reopening the debates with both parties. Hence, and seeing as both these exchanges and the sanction form will be part of the administrative file, the Litigation Chamber dismissed the complainants request to gain access to the sanction form and the written exchanges that followed with the defendant.
283. On 20 January 2022, the Litigation Chamber received a letter from the claimants, in which they claim that they have the right to obtain a copy of the sanction form and the subsequent exchanges with the defendant, in order to verify themselves whether no new elements were brought up by the latter. The claimants also argue that if the sanction form and subsequent exchanges will be part of the administrative file, and thus accessible in case of an appeal, there is no reason why they should not be granted access during the current proceedings. The claimants further claim, based on a press release by the defendant dd. 5 November 2021, that the Litigation Chamber has agreed to approve a Code of Conduct submitted by the defendant 6 months after its decision. The claimants argue this has not been subject to the debates during the proceedings, and thus request access to all written exchanges with the defendant following the sanction form, as well as the reopening of the debates on the Litigation Chamber’s competence to approve a code of conduct or validate an action plan.
284. On 27 January 2022, the Litigation Chamber acknowledged the reception of the claimant’s letter, and responded that their arguments will be taken into consideration in its deliberations.

Assessment by the Litigation Chamber

285. The Litigation Chamber first and foremost finds that it is not responsible and cannot be held accountable for public statements made outside of the proceedings by either or both of the parties involved during the Litigation Chamber’s deliberations on the merits.

286. Secondly, the Market Court has stated that the claimants do not have any say in the determination of the sanctions imposed by the Litigation Chamber⁶⁴. In this regard, Article 58.2.d of the GDPR grants supervisory authorities to order a controller or a processor to bring processing operations into compliance with the provisions of the GDPR, where appropriate, *in a specified manner and within a specified period*. This provision, read in conjunction with Article 100, §1, 9° of the Data Protection Act, must be interpreted in the sense that an action plan and the inherently involved monitoring of this action plan by the BE DPA, must be seen as one of the sanctions that can be imposed on a controller or processor. The action plan must therefore be seen as a corrective measures, with regard to which the claimants have no stake.
287. With regard to the defendant's request not to publish the decision, the Litigation Chamber reminds of the significant impact of the case, in view of the a large number of data subjects and organisations involved. Moreover, the Litigation Chamber notes that the request by the defendants was submitted after the closure of the debates, and that the defendant itself already published on the case on 5 November 2021. Having considered these elements, the Litigation Chamber considers not to give a positive reply to the defendant's request dd. 21 December 2021 not to publish the decision or issue public communications about the decision prior to the exhaustion of all appeals.

⁶⁴ Market Court, 1 December 2021, FOD Financiën v. GBA, nr. 2021/AR/1044, para. 7.3.4: "It is (certainly) not for a complainant to interfere in any way with the expediency, let alone the extent of a sanction. The complaint only concerns (and can only concern) an alleged infringement in such a way that the decision taken by the Dispute Resolution Chamber of the GBA in relation to the complaint - and in which it possibly imposes a sanction on the person concerned - is never an *ultra petita* judgment from the point of view of the complaint."

B. Reasoning

B.1. – Processing of personal data in the context of the Transparency and Consent Framework

288. In this section, the Litigation Chamber examines the concept of personal data as well as the question of whether personal data exists within the context of the Transparency and Consent Framework, designed and managed by IAB Europe⁶⁵ and is being processed⁶⁶.
289. For a proper understanding of this decision, the Litigation Chamber emphasises that the complainants indicated in their written submissions that they wished to limit themselves to the alleged breaches of the GDPR in the processing of personal data "in the TCF per se"⁶⁷. The Litigation Chamber will therefore not pass judgment in this section on processing responsibility with regard to the processing operations that take place in the context of the OpenRTB system.

B.1.1. – Presence of personal data within the TCF

290. European data protection law, including the GDPR, has always taken a broad view of personal data with the aim of ensuring a high level of data protection and safeguarding the fundamental rights and freedoms of data subjects. The broad interpretation of, inter alia, the concept of personal data and the notion of processing is a key element of the case law of the Court of Justice⁶⁸. The principle that personal data does not only relate to an identified, but also to an *identifiable* natural person was already established in 1981 by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data⁶⁹.
291. The GDPR unambiguously states that any information about an identified or identifiable natural person ("data subject") constitutes personal data. "Identifiable" should therefore be understood to mean the possibility of identifying a natural person directly or indirectly by means of an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person⁷⁰.
292. Furthermore, the GDPR provides that, to determine whether a natural person is identifiable, account should be taken of all means of which it can be reasonably assumed they will be

⁶⁵ See title B.1.1. – Presence of personal data within the TCF.

⁶⁶ See title B.1.2. - Processing of personal data within the TCF.

⁶⁷ Submission of the complainants dd. 18 February 2021, p. 2.

⁶⁸ C. DOCKSEY, H. HIJMANNS, "The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law", *EDPL Review*, 2019, p. 300.

⁶⁹ Article 2.a of the Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, B.S., 30 December 1993 (Convention 108).

⁷⁰ Article 4.1 GDPR.

used either by the data controller or by any other person to identify the natural person directly or indirectly, such as singling out⁷¹.

293. To determine whether resources can reasonably be expected to be used to identify the natural person, account should also be taken of all objective factors, such as the cost and time required for identification, taking into account the technology available at the time of processing and technological developments⁷².
294. Recital 30 GDPR clarifies that natural persons may be linked to online identifiers through their devices, applications, tools and protocols, such as Internet Protocol (IP) addresses, identification cookies or other identifiers. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.
295. The former Article 29 Working Party has already addressed the importance of a broad definition of personal data, in particular that a natural person can be considered identifiable when he/she can be distinguished from other members of the group and consequently treated differently⁷³.
296. This position is also taken by the Court of Justice. It is established case law that the content of the information that qualifies as personal data is not important⁷⁴ and that the criterion of identifiability must be interpreted flexibly. **As long as information, due to its content, purpose or effect, can be linked to an identified or identifiable natural person by means that can reasonably be used⁷⁵, regardless of whether the information from which the data subject can be identified is held entirely by the same controller or partly by another entity, this information should be considered personal data⁷⁶.**
297. The complainants argue in their submission in response that the TC String is a unique character string which is also written into a cookie as a unique identifier and is then stored on a user's device⁷⁷. Furthermore, the complainants take the view that IAB Europe collects

⁷¹ Recital 26 GDPR; the English text explicitly refers to "singling out" as one of the means of identifying a natural person. See also CJEU Judgment C-582/14 of 19 October 2016, *Patrick Breyer t. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para. 46, and FR. ZUIDERVEEN BORGESIUS, "Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection regulation", *Computer Law & Security Review*, vol. 32-2, 2016, pp. 256-271.

⁷² *Ibidem*.

⁷³ WP136 - Opinion 4/2007 on the concept of personal data, p.14; WP199 - Opinion 08.2012 providing further input on the data protection reform discussions, p. 5.

⁷⁴ Opinion of Advocate General Sharpston of 12 December 2013 in Joined Cases C-141/12 and C-372/12, Y.S., para. 45.

⁷⁵ CJEU Judgment C-434/16 of 20 December 2017, Nowak t. *Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 35.

⁷⁶ CJEU Judgment C-582/14 of 19 October 2016, *Patrick Breyer t. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, para. 43; CJEU Judgment C-434/16 of 20 December 2017, Nowak t. *Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 31; see also FR. ZUIDERVEEN BORGESIUS, "Singling out people without knowing their names - Behavioural targeting, pseudonymous data, and the new Data Protection regulation", *Computer Law & Security Review*, vol. 32-2, 2016, pp. 256-271; and FR. ZUIDERVEEN BORGESIUS, "The Breyer Case of the CJEU - IP Addresses and the Personal Data Definition", *EDPL*, 1/2017, pp. 130-137.

⁷⁷ Submissions of the complainants dd. 18 February 2021, para. 25.

additional information about users with the help of the TC String, including sensitive personal data within the meaning of Article 9 GDPR⁷⁸.

298. The defendant, on the other hand, refutes the allegations and states that the TC String does not contain any personal data⁷⁹ or any information directly or indirectly related to the so-called '*content taxonomy*'⁸⁰, which IAB Europe uses as a 'common language' to describe the content of a website⁸¹. Furthermore, the defendant takes the view that the TC String does not constitute a unique identifier, nor is it conceived for that purpose⁸².
299. Notwithstanding the foregoing, the defendant states that it must necessarily be possible to link the TC String with a user, but with the proviso that the link between the preferences conceived in the TC String and the user will be established only at a later stage, in particular in the context of the OpenRTB, and is therefore not covered by the Transparency & Consent Framework⁸³.
300. Based on the technical documentation of IAB Europe and IAB Tech Lab on the TCF protocol, the Inspection Service concludes that the TC String in itself does not *directly* identify users or devices, as the components that compose the TC String merely reflect technical information, namely whether or not an unidentified user has consented to purposes Y or Z, and whether *adtech vendors A and B* may process the personal data for the accepted purposes.
301. Specifically, a TC String consists of the following fields:
 - i. general metadata;
 - ii. a binary value for each of the purposes of the processing for which consent may be given;
 - iii. a binary value for each of the purposes of processing permitted by a legitimate interest;
 - iv. a binary value for each of the adtech vendors who may collect and process the user's personal data on the basis of his consent;
 - v. a binary value for each of the adtech vendors who may collect and process the user's personal data on the basis of a legitimate interest;
 - vi. any processing restrictions;
 - vii. special *opt-in* features in connection with the processing purposes;

⁷⁸ Submissions of the complainants dd. 18 February 2021, para. 26.

⁷⁹ Defendant's reply brief dd. 25 March 2021, para. 48.

⁸⁰ Defendant's reply brief dd. 25 March 2021, para. 51.

⁸¹ <https://iabtechlab.com/standards/content-taxonomy/>

⁸² Defendant's reply brief dd. 25 March 2021, para. 53.

⁸³ Defendant's reply brief dd. 25 March 2021, para. 54.

- viii. a field dedicated to processing purposes that do not fall under the TCF but are specific to the *publisher*;
- ix. consent to the processing on legal bases that are not covered by the TCF.

Assessment by the Litigation Chamber

302. While the Litigation Chamber understands that it is not conclusively established that the TC String, due to the limited metadata and values it contains, in itself allows for direct identification of the user, the Litigation Chamber notes that when the consent pop-up is accessed by script from a server managed by the CMP⁸⁴, it inevitably also processes the user's IP address, which is explicitly classified as personal data under the GDPR.
303. Indeed, Recital 30 GDPR states that natural persons may be linked to online identifiers through their devices, applications, tools and protocols, such as Internet Protocol (IP) addresses, identification cookies or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.
304. As soon as a CMP stores or reads the TC String on a user's device using a *euconsent-v2* cookie, the consent or objection to the processing on the grounds of legitimate interest, as well as the preferences of this user, can be linked to the IP address of the user's device. In other words, CMPs have the technical means to collect IP addresses (as indicated in their pop-up⁸⁵) and to combine all information relating to an identifiable person. The possibility of combining the TC String and the IP address means that this is information about an identifiable user⁸⁶.
305. In addition, identification of the user is possible by linking to other data that can be used by participating organisations within TCF, but also in the context of OpenRTB. In that regard, the Litigation Chamber emphasises that the parties in question are not one and the same, but participating organisations – CMPs and adtech vendors – who, as examined in more detail below⁸⁷ are obliged to disclose information enabling them to identify users to the defendant, upon simple request.

⁸⁴ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 58.

⁸⁵ See examples in the Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 99 ff.

⁸⁶ C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. Roca, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 50-51. The Litigation Chamber notes in this regard that, until this summer, if a 'globally stored' TC String was chosen, the CMPs could access the IAB Europe-managed *consensu.org* internet domain to verify whether a globally scoped consent had been given by the user, which involved the disclosure of the TC String values coupled with users' IP addresses to the CMPs, by IAB Europe. The defendant announced during the hearing that the globally scoped consents functionality would be deprecated.

⁸⁷ See para. 358 et seq. of this decision.

306. Therefore, the Litigation Chamber finds that the defendant has reasonable means at its disposal that it can use with respect to registered organisations participating in the TCF, and with which the defendant is able to identify directly or indirectly the user behind a TC String.
307. The Litigation Chamber also understands that the TCF is intended to and therefore inherently involves storing each user's combination of preferences in the form of a unique string in the TC String, in order to communicate those preferences to a large number of adtech vendors.
308. Indeed, the Litigation Chamber found from the inspection reports that adtech vendors as well as other participants within the wider OpenRTB ecosystem read the signal stored in a TC String in order to determine whether they have the required legal basis to process a user's personal data for the purposes to which the user has consented⁸⁸.
309. In this regard, the Litigation Chamber emphasises that it is sufficient that certain information is used to single out a natural person to be able to speak of personal data⁸⁹. Also, the purpose of the TC String, namely to capture the preferences of a specific user, leads *de facto* to the TC String being regarded as personal data.
310. **In other words, if the purpose of the processing is the singling out of persons, it may be assumed that the controller or another party has or will have at their disposal the means by which the data subject may reasonably be expected to be identified. To claim that individuals are not identifiable, when the purpose of the processing is precisely to identify them, would be a contradiction in terminis**⁹⁰.
311. Furthermore, the Litigation Chamber is of the opinion that the processing of these preferences has unmistakable consequences for the rights and interests of the data subjects, since these choices determine, among other things, which third parties will receive and process the personal data of the users in the context of the OpenRTB protocol⁹¹.
312. In view of the foregoing findings as well as the broad interpretation of the concept of personal data, as confirmed in the case law of the Court of Justice⁹², the Litigation Chamber concludes that the preferences of users in a TC String do constitute personal data, as these preferences relate to a singled out, identifiable natural person⁹³.

⁸⁸ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 75.

⁸⁹ WP136 - Opinion 4/2007 on the concept of personal data, p.14.

⁹⁰ WP136 - Opinion 4/2007 on the concept of personal data, p.16.

⁹¹ CJEU, judgment C-434/16 of 20 December 2017, Nowak *t. Data Protection Commissioner*, para. 39.

⁹² See para. 296 of this decision.

⁹³ CJEU, judgment C-434/16 of 20 December 2017, Nowak *t. Data Protection Commissioner*, para. 34.

B.1.2. - Processing of personal data within the TCF

313. The Inspection Service explains in its technical investigation reports that the TCF is necessarily based on three core components:
- i. a fully customisable user interface that allows TCF-registered *Consent Management Platforms* to collect the user's consent, any objections to processing based on a legitimate interest, and preferences regarding the purposes of processing and authorised *adtech vendors*;
 - ii. a *Global Vendors List* that includes partners approved by IAB Europe and specific information regarding their respective processing purposes and legal bases; and
 - iii. a standardised mechanism for requesting, storing and optionally sharing authorised *adtech vendors*, consents, objections and preferences through a dedicated API, a standard format for storing partners/consents, and a standardised data structure for transferring partner/consent status⁹⁴.
314. The complainants argue that the generation of the TC String corresponds to the automated creation of a unique string of characters associated with a specific user, through which his data exchange preferences are captured by the intervention of a CMP connected to the TCF⁹⁵.
315. Furthermore, the complainants refer to the sharing of the TC String with CMPs and other participants in the TCF. Specifically, they argue that the storage of a TC String in a specific *euconsent-v2* cookie, on a storage system chosen by the CMP or associated with the *consensu.org* internet domain managed by IAB Europe, also constitutes processing of user preferences.
316. The defendant, on the other hand, argues that there is no processing of personal data within the meaning of Section 4(2) GDPR in the context of the TCF, given its view that the TC String as such cannot be regarded as personal data.

Assessment by the Litigation Chamber

317. First and foremost, the Litigation Chamber refers to the definition of processing personal data as being any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

⁹⁴ Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 4; Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 58-59.

⁹⁵ Submissions of the complainants dd. 18 February 2021, para. 27.

disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction⁹⁶.

318. The TCF provides a standardised approach for collecting and exchanging personal data - i.e. consent, any objections, and preferences - from well-defined, already identified or at least identifiable users in a supposedly GDPR-compliant manner. The fact that participating organisations can directly identify data subjects with additional data such as an IP address from the TC String, which captures these consents, objections and preferences, means not only that the TC String can be considered personal data⁹⁷, but also that the participating organisations (*adtech vendors*) necessarily process personal data.
319. Taking into account the connection between the TCF and the OpenRTB protocol, the Litigation Chamber refers to the guidelines of the former Article 29 Working Party on Online Advertising, in which the Working Party noted that the methods of advertising based on surfing behaviour inherently involve the processing of personal data, as such advertising entails the collection of IP addresses and the processing of unique identifiers, so that data subjects can be followed online even if their real names are not known⁹⁸.
320. The Litigation Chamber understands that the *Transparency and Consent Framework* inherently entails the collection, processing, storage and subsequent sharing of users' preferences with other parties, whether or not in combination with additional personal data in the context of the OpenRTB.
321. Consequently, the Litigation Chamber finds that there is in fact processing of personal data within the meaning of Article 4.2 of the GDPR. This conclusion is also confirmed by consideration of the possibility that the TC Strings may at any time be linked to immediately identifiable information, whether provided by the data subject or not.

B.2. - Responsibility of IAB Europe for the processing operations within the Transparency and Consent Framework

322. IAB Europe states that it is neither data controller nor jointly responsible for the processing of personal data collected by the participating organisations in the context of the TCF.
323. However, the Litigation Chamber finds that this reasoning cannot be followed for several reasons. First of all, the broad interpretation by the Court of Justice of the concept of a data controller (B.2.1. - Broad interpretation of the concept of data controller by the Court of

⁹⁶ Art. 4.2) GDPR.

⁹⁷ See previous section, B.1.1. – Presence of personal data within the TCF.

⁹⁸ WP171 - Opinion 2/2010 on online behavioural advertising, 22 June 2010, p. 10, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_nl.pdf

Justice and the EDPB) must be applied. The fact that IAB Europe has a decisive influence on the purpose (B.2.2. - Determining the purposes of the processing of personal data within the TCF) and means (B.2.3. - Determining the means for processing personal data within a TCF) of the processing by imposing compulsory TCF parameters also needs to be taken into account.

B.2.1. - Broad interpretation of the concept of data controller by the Court of Justice and the EDPB

324. The GDPR defines a "data controller" as the entity that, alone or jointly with others, determines the purposes and means of the processing of personal data⁹⁹. This definition should be understood in the light of the legislator's objective of placing the main responsibility for the protection of personal data on the entity that actually exercises control over the data processing. This means that not only the legal qualification, but also the actual reality¹⁰⁰must be taken into account.
325. The EDPB has clarified that the concept of data controller refers to the influence of the data controller on the processing, based on a power of decision or monitoring of the processing activities. Such monitoring may be based on legal provisions, on an implicit power or on the exercise of a de facto influence¹⁰¹. In essence, determining the purposes and the means corresponds to deciding respectively the "why" and the "how" of the processing: given a particular processing operation, the controller is the actor who exerts such influence over the processing of personal data, thus determining why the processing is taking place (i.e., "to what end"; or "what for") and how this objective shall be attained (i.e. which means shall be employed to pursue the objective)¹⁰².
326. The power to determine the means and purposes of processing activities may first be linked to the functional role of an organisation¹⁰³. The responsibility may also be assigned on the basis of the contractual provisions between the parties involved, although these are not always decisive¹⁰⁴, or on the basis of an assessment of the actual control of a party. For example, determining the means and purposes may result from a decisive influence on the processing, in particular on why processing is carried out in a certain manner¹⁰⁵.

⁹⁹ Art. 4.7) GDPR

¹⁰⁰ L. A. BYGRAVE & L. TOSONI, "Article 4(7). Controller" in *The EU General Data Protection Regulation. A Commentary*, Oxford University Press, 2020, p. 148.

¹⁰¹ EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 20 et seq.

¹⁰² *Ibidem*, para. 35.

¹⁰³ D. De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, para. 362.

¹⁰⁴ D. De Bot, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context*, Wolters Kluwer, 2020, para. 363-365.

¹⁰⁵ EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 20.

327. In its Jehovah's Witnesses judgment¹⁰⁶, the Court of Justice gives a broad interpretation to the concept of a data controller. This judgment is relevant and applicable to the present case, as it clarifies that the definition of data controller must be interpreted broadly, in order to ensure 'effective and complete protection of the data subjects'¹⁰⁷, and that no access to the personal data concerned is required in order to qualify as a data controller¹⁰⁸. The Litigation Chamber quotes the relevant recitals of the aforementioned judgment below:

"65. As Article 2(d) of Directive 95/46 expressly provides, the term 'data controller' refers to the natural or legal person who, 'alone or jointly with others', determines the purposes and means of the processing of personal data. This concept does not therefore necessarily refer to a single natural or legal person and may involve several participants in such processing, each of whom is then subject to data protection provisions (see, to that effect, Judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, point 29).

66. Although the aim of that provision is to ensure effective and complete protection of data subjects through a broad definition of the term 'data controller', the existence of joint responsibility does not necessarily mean that the various participants in the processing of personal data are equally responsible. On the contrary, these participants may be involved in this processing at different stages and to different degrees, so that the assessment of the level of responsibility of each of them must take into account all the relevant circumstances of the particular case (see, to that effect, judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, points 28, 43 and 44).

67. In that regard, neither the wording of Article 2(d) of Directive 95/46, nor any other provision of that directive, permits the conclusion that the purposes and means of the processing must be determined by means of written guidelines or instructions from the data controller.

68. However, a natural or legal person who exercises influence over the processing of personal data for reasons of their own and thereby takes part in determining the purposes and means of processing may be regarded as a data controller within the meaning of Article 2(d) of Directive 95/46.

69. Moreover, the fact that several participants are responsible for the same processing under that provision does not presuppose that each of them has access to the personal data concerned (see, to that effect, Judgment of 5 June 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, point 38)."

¹⁰⁶ CJEU Judgment of 10 July 2018, *Tietosuojavaltuutettu et Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551.

¹⁰⁷ CJEU Judgment of 13 May 2014, *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others*, C-131/12, ECLI:EU:C:2014:317, paragraph 34; see also the discussion on the scope of the concept in C. DOCKSEY and H. HIJMAN, "The Court of Justice as a Key Player in Privacy and Data Protection", *European Data Protection Law Review*, 2019, issue 3, (300)304.

¹⁰⁸ CJEU Judgment of 10 July 2018, *Tietosuojavaltuutettu et Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551. See also EDPB - Guidelines 07/2020 on the concepts of data controller and processor in the GDPR, v2.0, 2021, para. 45.

328. It is therefore clear to the Litigation Chamber that the defendant does not necessarily have to process the personal data concerned itself, nor does it have to be able to grant itself any access to the personal data, in order for IAB Europe to be considered a data controller, as¹⁰⁹ in relation to a framework for which the defendant moreover charges an annual fee of 1.200 EUR to participating organisations¹¹⁰.
329. Furthermore, the impact or consequences of certain activities on the rights and freedoms of data subjects may also be taken into account when determining an organisation's responsibility. If it appears that an organisation plays a decisive role in the dissemination of personal data¹¹¹ or that the processing operations carried out under the influence of the organisation may substantially affect the fundamental rights to privacy and to the protection of personal data¹¹², that organisation should be regarded as a data controller.
330. *In this case*, the Litigation Chamber concludes that the participating parties, i.e. publishers and adtech vendors, would not be able to achieve the goals set by IAB Europe without the TCF. IAB Europe's framework thus plays a decisive role with regard to the collection, processing and dissemination of users' preferences, consents and objections, regardless of whether the defendant itself comes into contact with the aforementioned data.

B.2.2. - Determining the purposes of the processing of personal data within the TCF

331. Defining the purposes is the first condition for identifying the data controller of personal data¹¹³. Moreover, it is generally considered that defining the purposes of processing outweighs defining the means when it comes to establishing the responsibility of an organisation¹¹⁴. Incidentally, an erroneous designation by a data controller, such as a designation as a processor that is contradicted by the factual situation, is not binding on the court or supervisory authority¹¹⁵.
-

¹⁰⁹ CJEU Judgment of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI: EU:C:2017:796, para. 35; CJEU Judgment of 10 July 2018, *Tietosuojavaltiutettu et Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551, para. 69.

¹¹⁰ <https://iabeurope.eu/join-the-tcf/>

¹¹¹ CJEU Judgment of 13 May 2014, *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others*, C-131/12; ECLI: EU:C:2014:317, paragraph 36.

¹¹² CJEU Judgment of 13 May 2014, *Google Spain SL v. Agencia Española de protección de Datos (AEPD) and Others*, C-131/12; ECLI: EU:C:2014:317, para. 38.

¹¹³ Art. 4.7) GDPR; A. DELFORGE Titre 8. Les obligations générales du responsable du traitement et la place du sous-traitant" in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 9-12.

¹¹⁴ EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 20; L. A. BYGRAVE & L. TOSONI, "Article 4(7). Controller" in *The EU General Data Protection Regulation. A Commentary*, Oxford University Press, 2020, p. 150; B. VAN ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019, para 109-110; A. DELFORGE Titre 8. Les obligations générales du responsable du traitement et la place du sous-traitant" in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 12.

¹¹⁵ C. de TERWANGNE, "Titre 2. Définitions clés et champ d'application du RGPD" in *Le Règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, Bruxelles, 2018, para. 9-12.

332. The Inspection Service states that the *Transparency and Consent Framework* does not in itself constitute processing of personal data, but is a set of policy documents and technical specifications developed by IAB Europe and IAB Tech Lab¹¹⁶. The Litigation Chamber concurs with this statement by the Inspection Service.

333. However, the Litigation Chamber also found that personal data are processed in the context of the TCF, and more specifically the processing of user preferences, which CMPs record via a user interface and store using the TC String. To enable a standardised approach within the TCF, IAB Europe uses both policy documents and technical specifications:

- The *TCF Policies* consist of rules for participation that apply to publishers, *Consent Management Providers* (CMPs) and other adtech vendors.
- The technical specifications of the TCF, which provide a technical protocol with which participating organisations can immediately exchange the status of the information provided and the choices of the data subjects. These technical specifications are closely aligned with the *TCF Policies*, in order to provide the technical functionality needed to operationalise the TCF standard.

334. The defendant states in its defence that the processing of those preferences, in accordance with the rules imposed by the TCF on participating organisations, pursues the objective of enabling both website and app publishers and the advertising technology partners who support the targeting, delivery and measurement of advertising and content (adtech vendors) to obtain users' consent, to transparently disclose their processing purposes, and to establish a valid legal basis for the processing of personal data in order to provide digital advertising, among others¹¹⁷. This objective is also reflected in the *IAB Europe Transparency & Consent Framework Policies* (hereinafter "TCF Policies")¹¹⁸:

"ii. The goal of the Framework is to help players in the online ecosystem meet certain requirements of the ePrivacy Directive (and by extension its successor, the upcoming ePrivacy Regulation), and General Data Protection Regulation by providing a way of informing users about inter alia the storing and/or accessing of information on their devices, the fact that their personal data is processed, the purposes for which their personal data is processed, the companies that are seeking to process their personal data for these purposes, providing users with choice about the same, and signalling to third parties inter alia which information has been disclosed to users and what users' choices are."

¹¹⁶ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 9.

¹¹⁷ Defendant's reply brief, § 33.

¹¹⁸ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

335. It is also apparent from the documentation drawn up by the defendant that the purposes of the TC String are determined by IAB Europe:

*"A TC String's primary purpose is to encapsulate and encode all the information disclosed to a user and the expression of their preferences for their personal data processing under the GDPR. Using a Consent Management Platform (CMP), the information is captured into an encoded and compact HTTP-transferable string. This string enables communication of transparency and consent information to entities, or "vendors", that process a user's personal data. Vendors decode a TC String to determine whether they have the necessary legal bases to process a user's personal data for their purposes."*¹¹⁹

336. Although the Litigation Chamber emphasises that the purpose of the processing of the TC String must be distinguished from the purposes of the processing that takes place outside the TCF, such as the processing and exchange of the personal data that are part of a *bid request* in the context of OpenRTB, it finds that the TCF is offered *with the aim of indirectly promoting the use of OpenRTB*. In that respect, IAB Europe, in its capacity as *Managing Organisation*, acts as a hinge between TCF and OpenRTB, which, incidentally, was developed by IAB Tech Lab.

337. In support of its standpoint, the Litigation Chamber refers to the inventory of possible purposes that participating organisations may pursue within the context of the TCF. For example, the *TCF Policies* for CMPs, publishers and other *adtech vendors* respectively stipulate a mandatory list¹²⁰ with fixed and predefined Purposes¹²¹, Special purposes¹²², Features¹²³ and Special features defined by IAB Europe:

- Purpose 1 — Store and/or access information on a device
- Purpose 2 — Select basic ads
- Purpose 3 — Create a personalised ads profile
- Purpose 4 — Select personalised ads
- Purpose 5 — Create a personalised content profile
- Purpose 6 — Select personalised content
- Purpose 7 — Measure ad performance

¹¹⁹ Transparency and Consent String with Global Vendor & CMP List Formats v2.0, August 2019 (Exhibit 35), p. 8.

¹²⁰ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 26 ff.

¹²¹ The term "Purpose" refers to one of the defined purposes for processing of data, including users' personal data, by participants in the Framework that are defined in the TCF Policies or the Specifications.

¹²² "Special Purpose" means one of the defined purposes for processing of data, including users' personal data, by participants in the Framework that are defined in the TCF Policies or the Specifications for which Vendors declare a Legal Basis in the GVL and for which the user is not given choice by a CMP.

¹²³ "Feature" means one of the features of processing personal data used by participants in the Framework that are defined in the TCF Policies or the Specifications used in pursuit of one or several Purposes for which the user is not given choice separately to the choice afforded regarding the Purposes for which they are used.

- Purpose 8 — Measure content performance
- Purpose 9 — Apply market research to generate audience insights
- Purpose 10 — Develop and improve products
- Special Purpose 1 — Ensure security, prevent fraud, and debug
- Special Purpose 2 — Technically deliver ads or content
- Feature 1 — Match and combine offline data sources
- Feature 2 — Link different devices
- Feature 3 — Receive and use automatically-sent device characteristics for identification
- Special Feature 1 — Use precise geolocation data
- Special Feature 2 — Actively scan device characteristics for identification

338. The Litigation Chamber concludes from this that the purpose of the TC String, and in the broader sense of the processing of the TC String within the TCF as translated into the *TCF Policies*, has been established by IAB Europe.

B.2.3. - Determining the means for processing personal data within a TCF

339. Determining the means of processing is the second cornerstone of the concept of controllership. With regard to the means of processing, the EDPB makes a distinction between so-called "essential" and "non-essential" means. The choice of non-essential means may, in principle, be left to a processor without any reduction in the responsibility of the entity that determined the purposes¹²⁴.

340. "Essential means" are closely linked to the purpose and scope of the processing and are inherently reserved to the controller. Examples of essential means relate to the type of personal data processed ("what data are processed?"), the duration of the processing ("how long are they processed?"), the categories of recipients ("who has access to them?") and the categories of data subjects ("whose personal data are processed?"). "Non-essential means", on the other hand, mainly concern the practical aspects of the implementation, such as the choice of a particular type of hardware or software or the detailed security measures that can be left to the processor to decide¹²⁵.

341. It is established by the Litigation Chamber, and also confirmed by the defendant¹²⁶, that the *Transparency and Consent Framework* constitutes a framework of binding rules for the participating organisations with regard to the processing of user preferences. Participants

¹²⁴ EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 39-41.

¹²⁵ EDPB - Guidelines 07/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 40.

¹²⁶ Defendant's reply brief dd. 25 March 2021, para. 35.

in the TCF are assumed to accept the *Terms and Conditions for the IAB Europe Transparency & Consent Framework* (hereinafter "Terms and Conditions")¹²⁷ in order to register. By doing so, the Litigation Chamber finds that IAB Europe does not *only* monitor compliance with the TCF specifications and policies, as Managing Organisation. In addition, the defendant is *also* defining the rules applicable to the processing of TC Strings under the TCF, as well as imposing these rules on participating organisations.

342. In the following paragraphs, the Litigation Chamber will examine the extent to which essential means of processing the TC String are actually determined by IAB Europe.
343. Generation, modification and reading of the TC String – In the first place, the *TCF Technical Specifications*¹²⁸, the *IAB Europe Transparency and Consent Framework Implementation Guidelines* (hereinafter "TCF Implementation Guidelines")¹²⁹ and the *TCF Policies*¹³⁰ explain how CMPs can collect user approval, must generate a unique TC String, and need to store the value of the TC String.
344. Moreover, CMPs are obliged to register with IAB Europe in order to be able to generate a TC String¹³¹ and must follow the technical specifications developed by IAB Europe in cooperation with IAB Tech Lab regarding the API¹³² with which CMPs can generate the TC String and adtech vendors and publishers can read it¹³³. These specifications also show that the CMP API plays an essential role in the TCF, as it provides a standardised way for parties, such as the *publisher* or an *advertising vendor*, to access the users' preferences, which are managed by the *CMP*¹³⁴. The Litigation Chamber notes that the use of this API is mandatory when communicating between CMPs and adtech vendors.
345. With regard to the content of the TC String, the *TCF Technical Specifications* specify which information is included, including metadata such as the exact time the TC String was generated or modified.
346. In this regard, the Litigation Chamber refers to the *Wirtschaftsakademie* judgment, in which the Court of Justice held that the entity responsible for laying down, and a *fortiori* imposing, settings in relation to a data processing operation, thereby participates in determining the

¹²⁷ Terms and Conditions for the IAB Europe Transparency & Consent Framework ("Terms and Conditions") (Exhibit 33).

¹²⁸ Transparency and Consent String with Global Vendor & CMP List Formats v2.0, August 2019 (Piece 35).

¹²⁹ IAB Europe Transparency and Consent Framework Implementation Guidelines, August 2019 (Exhibit 36).

¹³⁰ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

¹³¹ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 76.

¹³² An API is a programming interface that allows you to "plug in" to an application to exchange data. An API is open and offered by the program owner. APIs are used in various fields of digital marketing to enable, for example, automated gateways for data exchange between programs such as Adwords, AdExchange and an agency or vendor. It can also be used by adtech vendors, agencies or software suppliers to automate advertising campaigns.

¹³³ Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 4.

¹³⁴ Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 6.

purposes and means of that processing and must therefore be regarded as the data controller¹³⁵.

347. Storage location - In their written evidence, the complainants argue that IAB Europe is responsible for managing the internet domain "consensu.org", to which the so-called *globally scoped* consent cookies¹³⁶ refer and which as such allows CMPs to consult and modify the TC Strings shared across multiple websites or applications.
348. In contrast, IAB Europe states in its submissions that although it has registered the *consensu.org* domain, there is no storage of the TC String on IAB Europe's servers to which that *consensu.org* domain refers. Indeed, IAB Europe delegates a subdomain of *consensu.org* to each registered CMP¹³⁷, which stores the TC String on the user's device using a *euconsent-v2* cookie and associates it with the *consensu.org* domain. According to the defendant, it is therefore only the CMP that generates and stores the TC String and the CMP's own servers that read out the TC String.
349. In order to establish the responsibility of IAB Europe for the processing of the TC Strings, it is necessary to determine to what extent the delegation of a sub-domain to a CMP by IAB Europe implies that the defendant establishes at least the means (and any purposes) of such processing.
350. The *TCF Technical Specifications* prescribe that sharing the TC String with CMPs should take place in two ways: either by storing the TC String in a storage system chosen by the CMP, if it is a service-specific consent¹³⁸; or by storing the TC String in a shared *globally scoped consent* cookie associated with the IAB Europe's *consensu.org* internet domain¹³⁹.
351. Based on the technical reports and the statements of the parties at the hearing, the Litigation Chamber concludes that a service-specific consent by means of a first-party *euconsent-v2* cookie has been established, and is therefore stored exclusively on the user's device. In this first scenario, the *euconsent-v2* cookie in question will therefore not be linked to the *consensu.org* domain, nor to the subdomain delegated to the CMP by IAB Europe.
352. However, in exceptional cases where the user's consent also applies to other websites, so-called *globally scoped* consent cookies, CMPs are required to store the relevant TC String

¹³⁵ CJEU Judgment of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI:EU:C:2017:796, paragraph 39: "In these circumstances, it must be judged that the administrator of a fan page on Facebook, such as Wirtschaftsakademie, by defining settings according to, in particular, its target audience and objectives for the management or promotion of its activities, participates in determining the purposes and means of the processing of personal data of visitors to its fan page".

¹³⁶ Which contain the TC Strings.

¹³⁷ More specifically, it concerns the subdomain <name of the CMP>.mgr.consensu.org. For example, for Onetrust this is <https://cookies.onetrust.mgr.consensu.org/>.

¹³⁸ In concrete terms, this means that the user's consent is only valid for the website visited, and for the purposes accepted and the adtech vendors approved.

¹³⁹ Transparency and Consent String with Global Vendor & CMP List Formats v2.0, August 2019 (Piece 35).

on the user's device by means of a *third-party* cookie, whereby the cookie is associated with the *consensu.org* domain¹⁴⁰. Only the CMPs are able to read the TC Strings on the user devices.

In this second scenario, each CMP is then given a separate sub-domain, assigned by IAB Europe via DNS delegation, where the consent cookie with the TC String is associated with the main domain *consensu.org* and its sub-domains. In concrete terms, this means that the scope of the globally scoped consent cookie includes both the domain *consensu.org* and the subdomains delegated to the CMPs.

354. According to the defendant, the globally scoped consent was only applied to a limited extent and IAB Europe stopped using and supporting it after the hearing. The Litigation Chamber takes note of this, but emphasises that this functionality also indicates that IAB Europe's responsibility goes beyond merely designing a framework.
355. The Litigation Chamber also considers that the defendant establishes the means of processing the TC String as well as the *euconsent-v2* cookie, both for the service-specific and for the globally-scoped consents. The fact that the TCF does not impose a specific mechanism for storing users' consent in the browser but merely recommends that CMPs use a *first-party* cookie does not preclude the finding that the defendant provides a list of possible mechanisms for linking the TC String to an individual user, of which the CMP API is the most common. More specifically, the Litigation Chamber notes that, in its policy document entitled '*Consent Management Platform API*', the defendant prescribes, among other things, the standardised way in which the various parties involved in the TCF can consult the preferences, objections and consents of users¹⁴¹:

How does the CMP provide the API?

Every consent manager MUST provide the following API function:

```
_tcfapi(command, version, callback, parameter)
```

The function `_tcfapi` must always be a function and cannot be any other type, even if only temporarily on initialization – the API must be able to handle calls at all times.

Secondarily, CMPs must provide a proxy for postMessage events targeted to the `_tcfapi` interface sent from within nested iframes. See the section on iframes for information on working with IAB SafeFrames.

What required API commands must a CMP support?

All CMPs must support four required API commands: '`getTCData`' , '`ping`' , '`addEventListener`' and '`removeEventListener`' .

¹⁴⁰ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), p. 79.

¹⁴¹ Consent Management Platform API v2.0, August 2019 (Exhibit 34), p. 6.

356. Categories of recipients of the TC String - The Litigation Chamber also rules that IAB Europe determines with whom the users' preferences are to be shared, by, among other things, providing a list of TCF-registered adtech vendors, the so-called *Global Vendors List* (GVL)¹⁴², as well as a list of permitted CMPs (*Global CMP List*)¹⁴³.
357. IAB Europe's documentation shows that publishers who wish to use the TCF are obliged to work with a TCF-registered CMP¹⁴⁴. In addition, the *TCF Implementation Guidelines* state that CMPs are obliged to collect consent and any objections for all purposes and partners chosen by the publisher, although this may be extended to all adtech vendors included in the GVL¹⁴⁵.
358. Retention period of the TC String - Finally, the two versions of the *TCF Policies* explicitly state that CMPs and participating adtech vendors must retain the record of the consent or objection, which is stored in the TC String, for as long as the processing is ongoing and make it available to the Managing Organisation, i.e. the defendant, upon the latter's simple request¹⁴⁶:

"8. Record Keeping

1. A CMP will maintain records of consent, as required under the Policies and/or the Specifications, and will provide the MO access to such records upon request without undue delay.
2. A CMP will retain a record of the UI that has been deployed on any given Publisher at any given time and make this record available to its Publisher client, Vendors, and/or the MO upon request.

[...]

15. Record Keeping

1. A Vendor must maintain records of consent, as required under the Policies and the Specifications, and will provide the MO access to such records upon request without undue delay.
2. A Vendor must maintain records of user identification, timestamps, and received Signals for the full duration of the relevant processing. A Vendor may maintain such records of user identification, timestamps, and Signals beyond the duration of the processing as required to comply with legal obligations or to reasonably defend or pursue legal claims, and/or for other processing allowed by law, under a valid legal basis, and consistent with the purposes for which the data was collected."

¹⁴² <https://iabeurope.eu/vendor-list/> and <https://iabeurope.eu/vendor-list-tcf-v2-0/>

¹⁴³ <https://iabeurope.eu/cmp-list/>

¹⁴⁴ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 21

¹⁴⁵ IAB Europe Transparency and Consent Framework Implementation Guidelines, August 2019 (Exhibit 36), p. 13.

¹⁴⁶ IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38), Articles 8 and 15; IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), Articles 8 and 15.

359. The Litigation Chamber therefore finds that IAB Europe bears the responsibility for defining the criteria by which the retention periods of the TC Strings can be determined.

360. It follows from the foregoing that, in addition to the purposes, IAB Europe does in fact determine the means of generating, storing and sharing the TC String by which the preferences, objections and consent of users are processed. The following elements are decisive according to the Litigation Chamber:

- i. IAB Europe defines how CMPs can collect consent or objections from users, generate a unique TC String, and store the value of the TC String;
- ii. IAB Europe, in collaboration with IAB Tech Lab¹⁴⁷, has developed the technical specifications of the API with which adtech vendors, among others, can access the preferences of the users, which are managed by the CMP, in a standardised way;
- iii. IAB Europe determines the storage location and method for both service-specific and globally scoped consent cookies;
- iv. IAB Europe manages the lists of registered CMPs and adtech vendors and therefore determines with which possible recipients the data relating to the TC String is communicated;
- v. IAB Europe determines the criteria by which the retention periods for TC Strings may be established and the way in which organisations participating in the TCF must make these TC Strings available to the *Managing Organisation*, i.e. the defendant.

361. Based on the foregoing explanations, the Litigation Chamber finds that **the defendant must be considered as data controller for the personal data processing with respect to the registration of the consent signal, objections and users' preferences by means of the TC String, in accordance with the policies and technical specifications of the Transparency & Consent Framework**.

B.3. - Joint controllership of publishers, CMPs and adtech vendors with regard to the means and purposes of the processing of personal data within the context of the TCF and of the OpenRTB

362. IAB Europe's responsibility does not exclude that there are other data controllers implementing the TCF and relying on the OpenRTB protocol, that have their own or shared responsibility for the personal data processing operations they perform.

¹⁴⁷ IAB Europe worked with IAB Tech Lab to determine the policies for the framework's rules. IAB Europe has also entrusted Tech Lab with the development as well as the hosting of the technical implementations and specifications of the TCF, due to their technological expertise.

B.3.1. - Joint processing responsibility

363. Article 26.1 of the GDPR states that joint responsibility exists when "two or more jointly determine the purposes and means of the processing". The Court of Justice specified that 'the existence of joint responsibility of the various actors does not necessarily mean that they are equally responsible for one and the same processing of personal data. On the contrary, those actors may be involved at different stages and to different degrees, so that the assessment of the level of responsibility of each of them must take account of all the relevant circumstances of the particular case'¹⁴⁸.
364. Again, the EDPB further explained that the assessment of joint processing responsibility should be based on a factual rather than a formal analysis of the actual impact on the purposes and means of processing¹⁴⁹.
365. First of all, the Litigation Chamber underlines that an *identical* decision does not necessarily have to exist in order to speak of joint processing responsibility; it is sufficient that the defined purposes are complementary to each other¹⁵⁰. The EDPB also emphasises that joint participation in the definition of the means and purposes may take the form of a common decision as well as result from different yet *converging* decisions of two or more entities regarding the purposes and essential means of a data processing operation¹⁵¹.
366. **Decisions may be considered to be convergent if they are complementary and necessary for the processing in a way that confers a tangible influence on the determination of the purposes and means of processing.** The question to be asked is whether the *intended* processing of personal data would be impossible without the participation of all parties, more specifically, whether the processing activities carried out by each party are inseparable and indivisible.
367. Both in its submissions and during the hearing, IAB Europe emphasised that the TCF and the OpenRTB system are completely independent from each other, in the sense that even without participation in the TCF, adtech vendors can freely process personal data within the context of the OpenRTB. On the other hand, the complainants have always referred to the

¹⁴⁸ CJEU Judgment of 10 July 2018, *Tietosuojavaltuutettu et Jehovan todistajat - uskonnollinen yhdyskunta*, C-25/17, ECLI:EU:C:2018:551, para. 66 and CJEU Judgment of 29 July 2019, *Fashion ID GmbH & Co. KG*, C-40/17, ECLI:EU:C:2019:629, para. 70.

¹⁴⁹ EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 52.

¹⁵⁰ Opinion of Advocate General Bobek in *Fashion ID*, C-40/17, ECLI: EU:C:2018:1039, paragraph 105: "Even though the specific commercial use of the data may not be the same, both the defendant and Facebook Ireland appear to be pursuing commercial purposes in general that appear to be complementary. Although there is no identical purpose, there is a unity of purpose, namely a commercial and an advertising purpose."

¹⁵¹ EDPB - Guidelines 7/2020 on the concepts of controller and processor in the GDPR, v2.0, 2021, para. 54.

inherent interconnectedness between OpenRTB and the TCF, which the defendant itself would confirm - according to the complainants - in the *TCF Implementation Guidelines*¹⁵².

368. The Litigation Chamber finds that the defendant's argument cannot be followed, given that the defendant repeatedly states in its submissions, that the reason for the existence of the TCF is precisely to bring the processing of personal data based on the OpenRTB protocol, among others, into conformity with the applicable regulations, including the GDPR and the ePrivacy directive. Although the Litigation Chamber understands that the TCF may also be used by *publishers* for other applications¹⁵³, whether or not in collaboration with CMPs, it is equally certain that the TCF was never intended to be a stand-alone, independent ecosystem.
369. On the contrary, the Litigation Chamber notes that the *Transparency and Consent Framework* includes policies and technical specifications that should enable website and application publishers (*publishers*) and adtech partners that support the targeting, delivery and measurement of advertising and content (*adtech vendors*) to disclose transparently their processing purposes, to establish a legal basis for the processing of personal data for the provision of digital advertising, and to obtain consent or identify objections of users¹⁵⁴.
370. **Thus, the Litigation Chamber finds that the decisions translated by IAB Europe into the provisions of the TCF policies and technical specifications, on the one hand, and the means and purposes determined by the participating organisations in relation to the processing - whether or not in the context of OpenRTB - of users' personal data, , on the other hand, must be regarded as convergent decisions¹⁵⁵. IAB Europe provides an ecosystem within which the consent, objections and preferences of users are collected and exchanged not for its own purposes or self-preservation, but to facilitate further processing by third parties (i.e. publishers and adtech vendors).**
371. As a result, the Litigation Chamber finds that IAB Europe and the respective participating organisations should be considered as joint controllers for the collection and subsequent dissemination of users' consent, objections and preferences, as well as for the related processing of their personal data, without the responsibility of participating CMPs and *adtech vendors* detracting from IAB Europe's responsibility.

¹⁵² <https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/TCF-Implementation-Guidelines.md#how-does-the-tc-string-apply-to-non-openrtb-situations>.

¹⁵³ Thus, the TCF can also be used for non-marketing-related purposes, e.g. audience measurement, performance measurement, etc.

¹⁵⁴ Defendant's reply brief dd. 25 March 2021, para. 33.

¹⁵⁵ See para. 365-366.

a. Consent Management Platforms (CMPs)

372. The CMPs ensure the technical implementation of consent banners through which data subjects indicate their choices regarding the processing of their personal data.
373. Specifically, CMPs have the function of storing users' consent, objections and preferences in the TC String, then storing the value in the form of a *euconsent-v2* cookie in the browsers used to visit the website, and finally providing an API to adtech vendors so that they can access the consent, objection and preference values for each individual user¹⁵⁶.
374. CMPs that wish to register in the IAB Europe TCF v2.0 should implement the standardised processing purposes and functionalities in their user interface to collect and store the preferences of the data subject in this regard¹⁵⁷. They must also comply with the applicable lawful principles, as set out in the IAB Europe TCF v2.0.
375. The Litigation Chamber has already established that the TC String in itself does not directly identify persons or devices. However, once the TC String is placed on the user's device, a CMP can assign a unique identifier to this TC String, i.e. the IP address of the device on which it is placed in the form of an *euconsent-v2* cookie¹⁵⁸.
376. To provide a CMP interface to users, publishers need to implement the CMP JavaScript code on their website. This code is then loaded directly from the CMP server or via the delegated subdomain. As a result of this HTTP(S) request, both the publisher's server and the CMP's server gain access to the IP address of the user visiting the website and seeing the CMP interface¹⁵⁹.
377. Access to that IP address allows CMPs to enrich the consent, objection and preferences contained in the TC String with other information already in their possession or in the possession of the publisher and linked to that same IP address. On this basis, the Litigation Chamber concludes that CMPs process a large number of personal data.
378. The Litigation Chamber assesses the extent to which the CMPs act as processors or as (joint) controllers in the following paragraphs.
379. According to the defendant, as laid down in its TCF Policies, CMPs are in principle considered to be processors¹⁶⁰. The Litigation Chamber disagrees with this view for the following reasons. The CMPs' main task is to develop and provide interfaces that can have

¹⁵⁶ C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 50.

¹⁵⁷ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 9 ff.

¹⁵⁸ See para. 302 et seq. of this decision. See also C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 50.

¹⁵⁹ *Ibidem*, p. 5.

¹⁶⁰ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 9 ff.

a direct impact on the choice of the data subjects. The CMPs therefore play a key role, not only in the context of the TCF, but also with regard to the processing of personal data under the OpenRTB. They are therefore obliged to comply with the data protection principles laid down in Article 5.1 of the GDPR (lawfulness, fairness and transparency of the processing of personal data).

380. Although the *TCF Policies* prohibit CMPs from giving any preference to particular adtech vendors on the *Global Vendors List*, and they must therefore in principle present all registered adtech vendors to users, unless otherwise provided by the *publishers*¹⁶¹, some authors note that a number of CMPs do not comply with this requirement. This is done either by imposing pre-selected adtech vendors on the *publishers* or by denying them the possibility of deviating from the full list of adtech vendors by default¹⁶².
381. It is also worth noting that CMPs have a wide margin of appreciation regarding the interface they offer to users. After all, the TCF policies impose only *minimum interface requirements* on participating CMPs¹⁶³, with the result that in practice the interfaces and compliance with the principles of fairness and transparency can vary greatly depending on which CMP the website and application *publishers* work with¹⁶⁴.
382. The foregoing findings lead the Litigation Chamber to conclude that CMPs play a significant role and therefore bear (joint) responsibility¹⁶⁵ with regard to the purposes and means of the processing of users' personal data within the TCF and the OpenRTB system.
383. The Litigation Chamber notes, however, that this conclusion does not mean that all CMPs must systematically be considered as joint-controllers together with IAB Europe and the website publishers, or that the scope of the joint-controllership is without boundaries. As explained earlier in this decision¹⁶⁶, the list of CMPs implementing the TCF is limitative¹⁶⁷ due to the mandatory registration and approval process with IAB Europe, as Managing Organisation. The Litigation Chamber finds the joint controllership established in relation to, respectively:
 - i. the website or application publisher,
 - ii. the specific CMP implemented by the publisher and providing the TCF interface to users,

¹⁶¹ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 9, § 8 and p. 10, § 11.

¹⁶² C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, pp. 57-59.

¹⁶³ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 61 ff.

¹⁶⁴ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 99-103.

¹⁶⁵ See para. 360 of this decision on the processing responsibility of IAB Europe for determining the recipients.

¹⁶⁶ See para. 102; 341; 344; 356-360; and 374.

¹⁶⁷ As of November 2021, the list of registered CMPs comprises 76 entries: <https://iabeurope.eu/cmp-list/>.

iii. IAB Europe, as Managing Organization.

In this respect, the Litigation Chamber underlines that appropriate arrangements must be made between the respective joint-controllers, in accordance with the requirements foreseen under Article 26 GDPR.

384. CMPs are in principle required under the TCF Policies — developed and administered by the defendant — to offer by default *all* TCF-registered adtech vendors in their interface. If CMPs apply the TCF Policies, the Litigation Chamber finds that the defendant is responsible for the essential means of processing, since IAB Europe determines the recipients of the personal data collected, and is thus jointly responsible for the transmission of the personal data, including some data in the *bid request*.
385. If, on the other hand, the CMPs deviate from the TCF Policies, the Litigation Chamber considers that this time the CMPs themselves act as data controllers in respect of the recipients of the personal data. To the extent that CMPs do not comply with the instructions imposed on them, they themselves are fully responsible¹⁶⁸, in line with Article 28.10 GDPR.
386. Finally, when the CMPs determine the list of recipients in accordance with the *publishers'* instructions, the Litigation Chamber finds that the *publishers* bear the main responsibility for the transfer of personal data to adtech vendors, without prejudice to IAB Europe's responsibility, without which the global list of participating *adtech vendors* would not exist in the first place.

b. Publishers

387. *Publishers* usually act as data controllers in the context of the TCF, as they are supposed to decide whether or not to cooperate with a registered CMP, and are also able to determine which adtech vendors are allowed to advertise on their website or in their application. In addition, *publishers* can exercise control over the legal ground for a specific processing purpose, and they can exclude certain processing purposes¹⁶⁹.
388. *Bid requests* are sent by *supply-side platforms* (SSPs), in their capacity as representatives of the *publishers*, to *demand-side platforms* (DSPs), which represent adtech vendors. The format and content (or "attributes") of such *bid requests* are determined in accordance with the technical specifications of the OpenRTB protocol, independently of the TCF.
389. As confirmed by the reports of the Inspection Service, IAB Europe is not involved in determining the attributes of a specific *bid request*. It is primarily the publishers of websites

¹⁶⁸ EDPB - Guidelines 7.2020 on the concepts of controller and processor in the GDPR, v2.0, para.150.

¹⁶⁹ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 21-22.

and applications who decide which attributes are included in a *bid request* and passed on to the adtech vendors.

390. A *bid request* contains at least a unique identifier for each *bid request* (*Bid ID*) and a unique identifier for the advertising space being auctioned (*Item ID*). In addition, a *bid request* will typically contain information about the user device, user details, website or application, and technical details about the advertising space (*Impression*)¹⁷⁰.
391. On the basis of the foregoing, the Litigation Chamber finds that the *bid request* contains the most personal data, and that these data are not processed by the defendant, but mainly by the *publishers*, the CMPs and the various *adtech vendors* who, in principle, are all required to comply with the values of the TC String, in accordance with the policies of the TCF.
392. To the extent that a *publisher* relies on a CMP that has implemented the TCF, the *bid request* will also contain a TC String indicating the preferences of the website visitor or application user. The Litigation Chamber is of the opinion that this can be considered not only as additional evidence that the TC String is indeed personal data, as it concerns information relating to an *identifiable* natural person¹⁷¹, but also demonstrates that the preferences stored in the TC String have a direct and significant effect on the subsequent processing activities.
393. Therefore, if a user knowingly or unknowingly gives his consent by means of an "accept all" button in a CMP interface, and both the website publisher and the CMP have not deviated from the full list of participating adtech vendors, this means that the personal data of the data subject will be shared with hundreds of third parties.
394. In line with its previous submission with regard to CMPs¹⁷², the Litigation Chamber rules that *publishers* also act as data controllers for the processing of users' preferences in a TC String as well as their personal data processed in a *bid request*.
395. In addition, the Litigation Chamber refers to Article 23.5 of the *TCF Policies*, which prohibits *publishers* from changing the processing purposes, or giving CMPs any instruction to that effect¹⁷³.
396. Therefore, insofar as the *publishers* decide not to deviate from the proposed default list of *adtech vendors* and accept all the proposed processing purposes, the Litigation Chamber also considers that IAB Europe is acting as a joint data controller with the *publishers* in

¹⁷⁰ Technical Analysis Report of the Inspection Service, 4 June 2019 (Exhibit 24), pp. 12-13.

¹⁷¹ See para. 291 et seq. of this decision.

¹⁷² See para. 382 et seq. of this decision.

¹⁷³ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 22-23.

respect of the recipients of the TC String as well as the processing purposes for which the users' personal data will be processed.

c. Adtech vendors

397. The Litigation Chamber has already determined that IAB Europe bears responsibility with regard to defining the various processing purposes under the TCF¹⁷⁴.
398. When registering for TCF v2.0, adtech vendors must also choose the intended processing purposes and possible bases, based on a predetermined, fixed list of purposes.
399. In this sense, the Litigation Chamber finds that the adtech vendors, together with the defendant, are jointly responsible for the processing operations that take place within the context of the OpenRTB for the processing purposes foreseen under the TCF and in accordance with the preferences, objections and consents collected within the TCF. The latter aspect, however, does not affect the role that adtech vendors themselves play when they specify the purposes for which they themselves wish to process the personal data contained in a *bid request*, or for subsequent data processing not provided for under the TCF¹⁷⁵.
400. Moreover, the Litigation Chamber makes it clear that, similarly to the CMPs, adtech vendors are also required to register with the TCF in order to benefit from it. This means that the joint-controllership is limited to the registered adtech vendors¹⁷⁶.

d. Assessment by the Litigation Chamber

401. This factual analysis of the role of CMPs, publishers and adtech vendors shows that the decisions on determining the purposes and means of the processing activities carried out by the defendant within the context of the TCF (which aim to bring the processing activities carried out by the aforementioned participating organisations in line with the GDPR and the ePrivacy Directive) complement the decisions regarding the purposes and means of the processing activities carried out by the participating organisations under the OpenRTB and should thus be regarded as convergent decisions.
402. **This leads the Litigation Chamber to the conclusion that the defendant as well as the CMPs, publishers and participating adtech vendors should be regarded as joint data controllers for the collection and dissemination of users' preferences, objections and consent and for the subsequent processing of their personal data.**

¹⁷⁴ See para. 331 et seq. of this decision.

¹⁷⁵ WP171 - Opinion 2.2010 on Online Behavioural Advertising, pp. 10-11.

¹⁷⁶ <https://iabeurope.eu/vendor-list-tcf-v2-0/>.

B.4. On the alleged breaches of the General Data Protection Regulation

B.4.1 - Lawfulness and fairness of processing (Art. 5.1.a and 6 GDPR)

403. With regard to the lawfulness and fairness of the processing, the Litigation Chamber distinguishes two processing activities: on the one hand, the capture itself of the consent signal, objections and preferences of users in the TC String by the CMPs (a), and, on the other hand, the collection and dissemination of the users' personal data by the participating organisations (b).

a. Registration of the consent signal, objections and users' preferences by means of the TC String

404. The Litigation Chamber finds that users are not informed anywhere of the lawful basis for the processing of their own, individual preferences in relation to purposes and permitted adtech vendors by CMPs.

405. The underlying reasoning of the defendant in this regard is that the TC String is not personal data and therefore no basis for its processing is required.

406. As already established, the Litigation Chamber does not agree with the defendant's position¹⁷⁷. The Litigation Chamber has established that the generation and dissemination of the TC String does involve the processing of personal data.¹⁷⁸ Consequently, this processing must in any case be based on one of the exhaustively listed processing grounds under Article 6 of the GDPR. For this reason, the Litigation Chamber will consider the question of whether one of the legal bases of Article 6 GDPR can be relied on.

407. First of all, the Litigation Chamber finds that neither the *TCF Policies* nor the *TCF Implementation Guidelines* mention an obligation on the part of the CMPs to obtain the unambiguous consent of users before capturing their preferences in a TC String, which is placed on the end devices of users thanks to a euconsent-v2 cookie. Furthermore, users are never informed about the processing of their preferences by the TC String, with whom their preferences are shared, nor how long their preferences are stored. Since the visitors' consent is never asked, Article 6.1.a *de facto* does not apply as a legal basis for this processing.

408. In addition, the Litigation Chamber points out that Article 6.1.b is *prima facie* not applicable to the processing of user preferences and the TC String. In the majority of the cases, even if there were a contractual relationship between the users and the publisher, the data processing involved under the TCF would still not meet the requirement of objective

¹⁷⁷ See *supra* B.1.1. – Presence of personal data within the TCF.

¹⁷⁸ See *supra* B.1.2. - Processing of personal data within the TCF.

necessity for the provision of online services by the publishers to the users concerned (in particular for processing for the purposes of personalisation of content and for advertising based on surfing behaviour)¹⁷⁹.

409. In the absence of any contractual relationship between the data subjects and CMPs or IAB Europe, as well as an unambiguous consent given by the users for placing a euconsent-v2 cookie, the Litigation Chamber must assess whether Article 6.1.f (legitimate interest) could serve as legal basis: does the legitimate interest pass the threefold test of the CJEU and, if so, could Article 6.1.f GDPR serve as a basis for this preliminary processing of the users' preferences by CMPs, in accordance with the means and purposes as set out by IAB Europe in its *TCF Policies* and *TCF Implementation Guidelines*?
410. In order to rely on Article 6.1.f GDPR as a legal ground for the processing of personal data, the legitimate interest of the controller or third parties, which is closely related to (yet distinct from) the concept of processing purpose, must be balanced against the interests or fundamental rights and freedoms of the data subjects. Whereas 'purpose' refers to the specific reason why the data are processed, *i.e.* the aim or intention of the data processing, the notion of interest is linked to the broader stake that a controller may have in the processing, or the benefit that the controller — or a third party, which must not necessarily qualify as a co-controller in respect of the data processing — derives from the processing¹⁸⁰.
411. Pursuant to Article 6.1.f of the GDPR and the case law of the Court of Justice, three cumulative conditions must be met in order for a controller to be able to validly rely on this grounds for lawfulness, "*namely, firstly, the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, secondly, the necessity of processing the personal data for the purposes of the legitimate interest pursued and, thirdly, the condition that the fundamental rights and freedoms of the data subject are not prejudiced*" (Rigas judgment¹⁸¹).
412. In order to be able to invoke the ground for lawfulness of "legitimate interest" under Article 6.1.f of the GDPR, the controller must demonstrate, in other words, that:
 - 1) the interests it pursues with the processing can be recognised as legitimate (the 'purpose test');

¹⁷⁹ EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8 October 2019, para. 23 *et seq.*, para. 52 *et seq.* and para. 57 *et seq.*, <https://edpb.europa.eu>. This is a situation different from the pending case before the Court of Justice C-446/21, Maximilian Schrems vs. Facebook Ireland Ltd.

¹⁸⁰ CJEU Judgment of 11 December 2019, *TK v. Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 44.

¹⁸¹ CJEU Judgment of 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde t. Rīgas pašvaldības SIA "Rīgas satiksme"*, C-13/16; ECLI: EU:C:2017:336, paragraphs 28-31. See also CJEU Judgment of 11 December 2019, *TK v. Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 40.

- 2) the processing envisaged is necessary for the purposes of achieving those interests (the "necessity test"); and
 - 3) the balancing of these interests against the interests, fundamental freedoms and rights of data subjects weighs in favour of the data controller or a third party (the "balancing test").
413. As regards the first condition, the Litigation Chamber considers that the purpose of capturing users' approval and preferences in order to ensure and be able to demonstrate that users have validly consented to or not objected to the processing of their personal data for advertising purposes may be considered to be carried out for a legitimate interest.
414. The interest pursued by the defendant as the data controller may, in accordance with recital 47 of the GDPR, be regarded as legitimate in itself. More specifically, the possibility of storing the preferences of users¹⁸² is an essential part of the TCF and the Litigation Chamber notes that this is done in the legitimate interest of the defendant as well as of third parties involved, such as the participating *adtech vendors*.
415. Thus, the first condition set out in Article 6.1.f of the GDPR is fulfilled.
416. In order to fulfil the second condition, it must then be demonstrated that the processing is necessary for the achievement of the purposes pursued. This means, in particular, that the question must be asked whether the same result can be achieved by other means without processing personal data or without processing that is unnecessarily burdensome for the data subjects.
417. In view of the objective of enabling both website or application publishers and participating adtech providers to communicate the purposes of their processing in a transparent manner, to establish a valid legal basis for the processing of personal data for the purpose of providing digital advertising, and to obtain consent — or to identify whether an objection has been raised to the processing of data based on their legitimate interest¹⁸³, the Litigation Chamber must verify whether the personal data included in the TC String are limited to what is strictly necessary to capture the consent, objections and preferences of a specific user.
418. This second condition is also met by compliance with the principle of data minimisation (Article 5.1.c of the GDPR). The Litigation Chamber notes that the information processed in a TC String¹⁸⁴ is limited to data that are strictly necessary to achieve the intended purpose.

¹⁸² Including the collection of a valid consent prior to the processing of personal data, or the possibility for the users to object to a processing based on Article 6.1.f GDPR at the time of the collection of personal data.

¹⁸³ IAB Europe Transparency & Consent Framework - Policies, Version 2020-11-18.3.2a, p. 5, <https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/>

¹⁸⁴ See para. 300 and 301 of this decision.

In addition, based on the documents in this file and the parties' defences, the Litigation Chamber has not been able to establish that the TC String is retained indefinitely.

419. In order to verify whether the third condition of Article 6.1.f of the GDPR — the so-called "balancing test" between the interests of the data controller, on the one hand, and the fundamental freedoms and rights of the data subject, on the other hand — can be met, the reasonable expectations of the data subject must be taken into account in accordance with recital 47 of the GDPR. In particular, it should be evaluated whether the data subject "may reasonably expect, at the time and in the context of the collection of personal data, that processing may take place for that purpose"¹⁸⁵.

420. This is also emphasised by the Court of Justice in its judgment "Asociația de Proprietari bloc M5A-ScaraA"¹⁸⁶, in which it states:

"Also relevant for this are the data subject's reasonable expectations that his or her personal data will not be processed when, in the given circumstances of the case, the data subject cannot reasonably expect further processing of the data."

421. In this regard, the Litigation Chamber finds it remarkable that no option is offered to users to completely oppose the processing of their preferences in the context of the TCF. Regardless of which choice they make, the CMP will generate a TC String before linking it to the user's unique User ID through a euconsent-v2 cookie placed on the data subject's end device.

422. Moreover, since users are not informed of the installation of an euconsent-v2 cookie on their terminal device, whether or not they agree with the purposes and adtech vendors offered by the CMP, and moreover they are not informed of their right to object to such processing, the Litigation Chamber finds that the last condition of Article 6.1.f of the GDPR is currently not met.

423. The severity of the breach of the data subject's rights and freedoms is also an essential element of the assessment under Article 6.1.f GDPR. The result of this assessment depends on the particular circumstances of a specific case¹⁸⁷. In this context, according to the Court of Justice, particular account should be taken of 'the nature of the personal data concerned, in particular their potentially sensitive nature, and of the nature and specific way in which they are processed, in particular the number of persons having access to them and the way in which they acquire such access'¹⁸⁸. In this context, the Litigation Chamber

¹⁸⁵ Recital 47 of the GDPR.

¹⁸⁶ CJEU Judgment of 11 December 2019, *TK v. Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 58.

¹⁸⁷ *Ibidem*, para. 56.

¹⁸⁸ CJEU Judgment of 11 December 2019, *TK v. Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 57.

emphasises the large number of participating organisations that are given access to the TC String, in addition to the reduced control by the data subjects over the nature and the scope of the processing of their personal data by these organisations.

- 424. In the absence of a valid legal basis, the Litigation Chamber rules that the data processing in the context of the TCF in its current format, whereby CMPs capture the preferences of online users in a TC String, does not comply with Article 6 of the GDPR.**
- 425. It is therefore undeniable to the Litigation Chamber that IAB Europe, as *Managing Organisation* for the TCF, has failed to provide a legal basis for the processing of user preferences in the form of a TC String and has therefore breached article 6 GDPR.**

b. Collection and dissemination of personal data in the context of the RTB

426. It is in no way disputed that the TCF is aimed at capturing, through the interfaces offered by the CMPs, the consent of users or their lack of objection to the legitimate interests of the participating adtech vendors.
427. For the record, the Litigation Chamber emphasises that these two bases relate to processing activities that take place under the RTB, in accordance with the OpenRTB protocol.
428. However, the Litigation Chamber finds that none of the legal grounds proposed and implemented by the TCF can be lawfully invoked by TCF participants. First of all, the Litigation Chamber considers that the consent of the data subjects obtained through CMPs is not legally valid (*i*) nor is the (pre)contractual necessity applicable (*ii*). Furthermore, the Litigation Chamber finds that the legitimate interest does not meet the threefold test of the CJEU (*iii*). Thus, Article 6 of the GDPR is infringed.
 - (*i*) - Consent is not a valid basis for the processing operations in the OpenRTB facilitated by the TCF
429. In order to ensure that *publishers* and *adtech vendors* comply with the stricter transparency and consent requirements under the GDPR with respect to the processing of personal data in the context of OpenRTB (or RTB in general), CMPs provide a relatively standardised interface for users to choose whether to consent or object to the transfer of their personal data to hundreds of third parties at once, for specified purposes.
430. On the basis of the documents in this file, the Litigation Chamber understands that the participants can pursue one or more purposes from the 12 standardised purposes that the

TCF makes available to participating adtech vendors and that are offered to users by means of the CMPs¹⁸⁹.

431. However, the system of CMPs poses problems on several levels, with the result that the consent obtained by these CMPs (via the TCF) for the processing carried out in the context of the OpenRTB is not legally valid in light of Article 7 GDPR.
432. In order to be used as a legitimate basis, consent under Article 7 of the GDPR must meet strict conditions. However, for the reasons set out below, the Litigation Chamber finds that the consent collected by CMPs and publishers in the current version of the TCF is insufficiently free, specific, informed and unambiguous.
433. First of all, the Litigation Chamber finds that the proposed processing purposes are not sufficiently clearly described, and in some cases are even misleading¹⁹⁰. By way of example, the Litigation Chamber finds that purpose 8 ("Measure content performance") and 9 ("Apply market research to generate audience insights")¹⁹¹ provide little or no insight into the scope of the processing, the nature of the personal data processed or for how long the personal data processed will be retained if the user does not withdraw his consent.
434. Furthermore, based on the documents in the file, the Litigation Chamber understands that the *user interface* of the CMPs does not provide an overview of the categories of data collected, which makes it impossible for users to give their informed consent.
435. The Litigation Chamber also notes that the TCF makes it particularly difficult for users to obtain more information about the identity of all data controllers to whom they give consent to process their data for certain purposes before obtaining their consent. In particular, the recipients for whom consent is obtained are so numerous that users would need a disproportionate amount of time to read this information, which means that their consent can rarely be sufficiently informed.
436. Moreover, the information CMPs provide to users remains too general to reflect the specific processing operations of each vendor, thus preventing the necessary granularity of consent.
437. In addition, the Litigation Chamber takes the view that the enrichment of the data in a *bid request* with personal data already held by the *adtech vendors* and the relevant *Data Management Platforms* means that users cannot possibly be properly informed, since the TCF in its current format does not provide for participating organisations to indicate what

¹⁸⁹ For an overview of these TCF purposes, see para. 337 of this decision.

¹⁹⁰ See para. 465 et seq. of this decision.

¹⁹¹ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 34-36.

personal data they already hold and what processing operations they already perform with these data.

438. Finally, the Litigation Chamber finds that consent, once obtained by CMPs, cannot be withdrawn by users as easily as it was given, as required by Article 7 GDPR. First of all, the Litigation Chamber notes that under the *TCF Policies*, *adtech vendors* are required to comply with a user's consent signals in real time¹⁹², while no measure is provided to ensure that *adtech vendors* cannot continue their processing based on a previously received consent signal. After all, the TCF does not provide for proactive communication of the changed consent signals to the *adtech vendors*. In addition, *adtech vendors* can in principle no longer access the personal data of the data subject after the latter has withdrawn his consent, which also means that they cannot identify the user for whom consent has been withdrawn as such, with the result that the *adtech vendors* will continue to process the personal data of the user in question¹⁹³.
 439. Indeed, the Litigation Chamber understands that CMPs are at the intersection between users and participating *adtech vendors*, who receive their personal data and then process them for their own purposes. Such a configuration therefore means that the withdrawal of a consent via a CMP will only take effect as soon as the vendor concerned reads the new values in the modified TC String via the CMP API. In other words, the withdrawal of consent is never immediate and thus cannot be considered effective.
 440. Therefore, the Litigation Chamber concludes that Article 6.1.a GDPR does not constitute a valid legal basis for the processing and dissemination of personal data in the context of the OpenRTB, insofar as such consent was obtained in accordance with the TCF in its current format.
- (ii) - The legitimate interest of the participating organisations does not outweigh the protection of the fundamental rights and freedoms of the data subjects.
441. The question is then to what extent the organisations participating both in the TCF and the OpenRTB (*adtech vendors*) can legitimately rely on Article 6.1.f GDPR for the predefined processing purposes that entail targeted advertising or profiling of the users, as opposed to non-marketing related purposes such as audience measurement and performance measurement.
 442. As referred to previously¹⁹⁴, the assessment of the legitimate interests should be done on the basis of the three steps approach established by the Court of Justice. This assessment

¹⁹² IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2.a (Exhibit B.13), p. 14.

¹⁹³ For more information, see: M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", *German Law Journal*, 31 July 2021, p. 26.

¹⁹⁴ See para. 411 et seq.

shall be conducted by the data controllers prior to a processing operation based on Article 6.1.f GDPR. They determine the means and purposes of the intended personal data processing activities and are thus able to apply appropriate safeguards to prevent a disproportionate impact on the data subjects. In case of several controllers which are jointly responsible, the principles of accountability and transparency require that the assessment should be performed jointly by all the data controllers involved in the processing.

443. As stated by the Article 29 Working Party, both positive and negative consequences should be taken into consideration when assessing the impact of the processing, which must be necessary and proportionate to achieve the legitimate interests pursued by the data controllers or a third party. Such consequences may include “potential future decisions or actions by third parties, and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject”¹⁹⁵.
444. With regard to the purpose test, in particular whether the interests pursued by publishers and adtech vendors in processing personal data can be recognised as legitimate, the Litigation Chamber understands that the participating organisations have an interest in collecting and processing users' personal data in order to be able to offer tailor-made advertisements.
445. Based on the case law of the Court of Justice and the guidelines of the EDPB, the Litigation Chamber finds that the notion of legitimate interest can have a broad scope, with the understanding that an interest invoked by a data controller must be sufficiently specific, existent, current, and not hypothetical¹⁹⁶.
446. In this regard, the Litigation Chamber can only note that the proposed processing purposes are described in general terms, with the result that it is not easy for users to assess to what extent the collection, dissemination and processing of their personal data are necessary for the intended purposes, insofar as these are also understood by the users.
447. In order to be relevant, a legitimate interest must be in accordance with applicable EU and national law; sufficiently specific and clearly articulated to allow the balancing test to be carried out, and represent a real and present interest. Hence, merely invoking a legitimate interest in the processing of personal data is not sufficient; the outcome of the balancing test will determine whether Article 6.1.f GDPR can be relied upon¹⁹⁷.

¹⁹⁵ Article 29 Working Party – Opinion 06.2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95-46-EC (WP217), p. 37.

¹⁹⁶ CJEU Judgment of 11 December 2019, *TK v. Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 44.

¹⁹⁷ *Ibidem*, p. 25.

448. The *TCF Policies* do not foresee an obligation for the CMPs to explain the legitimate interests at stake in clear terms to the users. Instead, the specific user interface (UI) requirements contained in the *TCF Policies* for framework UIs in connection with legitimate interests, only require from the CMPs that a secondary information layer be provided¹⁹⁸, allowing the users to:

- i. see information about the fact that personal data is processed, and the nature of the personal data processed (e.g. unique identifiers, browsing data);
- ii. see information about the scope of the legitimate interest processing and scope of any objection to such processing;
- iii. access settings within the Framework UI to object to processing of their personal data on the basis of a legitimate interest;
- iv. review the list of processing purposes including their standard name and their full standard description, as defined in Appendix A of the *TCF Policies*, and to provide users with a way to see which vendors are processing their data for each of the purposes on the basis of a legitimate interest;
- v. exercise their right to object, either with respect to each adtech provider whose processing is based on legitimate interest or, separately, for each purpose pursued by adtech providers on the basis of legitimate interest;
- vi. review the list of named vendors, their purposes and legal bases, and find a link to each vendor's privacy policy.

449. By way of example, the Litigation Chamber refers to the definitions for processing purpose 5 (Create a personalised content profile), in Appendix A of the *TCF Policies*¹⁹⁹:

¹⁹⁸ IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2a, pp. 67-68.

¹⁹⁹ IAB Europe Transparency & Consent Framework Policies v2020-11-18.3.2a, p. 32.

Purpose 5 - Create a personalised content profile

Number	5
Name	Create a personalised content profile
Legal text	To create a personalised content profile vendors can: <ul style="list-style-type: none"> • Collect information about a user, including a user's activity, interests, visits to sites or apps, demographic information, or location, to create or edit a user profile for personalising content. • Combine this information with other information previously collected, including from across websites and apps, to create or edit a user profile for use in personalising content.
User-friendly text	A profile can be built about you and your interests to show you personalised content that is relevant to you.
Vendor guidance	<ul style="list-style-type: none"> • Allowable Lawful Bases: Consent, Legitimate Interests • Content refers to non-advertising content. Creating a profile for advertising personalisation, such as, paid cross-site content promotion and native advertising is <i>not</i> included in Purpose 5, but the corresponding ad-related Purpose 3 • When combining information collected under this purpose with other information previously collected, the latter must have been collected with an appropriate legal basis. • This purpose is intended to enable these processing activities: <ul style="list-style-type: none"> ◦ Associate data collected, including information about the content and the device, such as: device type and capabilities,

32

450. Notwithstanding the fact that the TCF Policies state that they establish minimum requirements for language, design and other elements in the Framework UI, intended to align with legal requirements of EU privacy and data protection law, the Litigation Chamber also notes that the general rules and requirements for framework UIs further specify that:

"b. When providing transparency about Purposes and Features, the Framework UI must do so only on the basis of the standard Purpose, Special Purpose, Feature, and Special Feature names and definitions of Appendix A as they are published on the Global Vendor List or using Stacks²⁰⁰ in accordance with the Policies and Specifications. UIs must make available the standard legal text of Purposes, Special Purposes, Features, and Special Features of Appendix A but may substitute or supplement the standard legal definitions with the standard user friendly text of Appendix A so long as the legal text remains available to the user and it is explained that these legal texts are definitive."

451. The Litigation Chamber interprets these general rules as prohibiting CMPs and publishers participating to the TCF from further explaining to the data subjects, in a clear and user-friendly manner, both the pursued legitimate interests as well as the reasons for believing

²⁰⁰ Stacks are, in essence, combination of different processing purposes.

that their interests are not overridden by the interests or fundamental rights and freedoms of the data subjects²⁰¹.

452. Although, in the context of the present case, the Litigation Chamber does not express an opinion on whether an economic interest²⁰² can be regarded as a legitimate interest within the meaning of Article 6.1.f of the GDPR, it considers that the lack of specificity of the stated purposes means that the first condition for *specific* lawful processing is not met with the standard descriptions of the processing purposes and pursued interests, as imposed by the *TCF Policies*.
453. In the context of the necessity test, which aims to determine whether the intended processing operations are necessary for achieving the interests pursued, the question should be asked whether the legitimate interests pursued by the processing of data could not reasonably be achieved just as effectively by other means with less interference with the fundamental freedoms and rights of data subjects, in particular their right to respect for their privacy and their right to the protection of personal data as guaranteed by Articles 7 and 8 of the Charter²⁰³.
454. The Court of Justice has also clarified that the condition of necessity of processing must be examined in relation to the principle of data minimisation laid down in Article 5.1.c GDPR²⁰⁴. In other words, according to the EDPB, it is necessary to consider whether other, less invasive means are available to achieve the same objective.
455. *In this case*, the Litigation Chamber understands that no safeguards are provided to ensure that the personal data collected and disseminated are limited to information that is strictly necessary for the purposes intended²⁰⁵.
456. In the absence of measures that adequately demonstrate that no inappropriate personal data are being disseminated, the Litigation Chamber is forced to decide that the second condition has not been met.
457. With regard to the balancing test, in particular whether the interests pursued by the *adtech vendors* outweigh the fundamental freedoms and rights of the data subjects, the

²⁰¹ Article 29 Working Party – Opinion 06.2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95-46-EC (WP217), p. 47.

²⁰² As opposed to the interest pursued by capturing the users' choices in a TC String, as discussed in para. 404 et seq.

²⁰³ CJEU Judgment of 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde t. Rīgas pašvaldības SIA "Rīgas satiksme"*, C-13/16; ECLI: EU:C:2017:336, para. 47.

²⁰⁴ *Ibidem*, para. 48.

²⁰⁵ In this respect, some authors argue that there are alternatives to RTB, in which only minimal information about the user is communicated. See M. VEALE, FR. ZUIDERVEEN BORGESIUS, "Adtech and Real-Time Bidding under European Data Protection Law", German Law Journal, 31 July 2021, pp.19 et seq. The authors refer in particular to the browser plug-in Adnostic, which was developed 10 years ago and builds up a profile based on the user's surfing behaviour in order to target advertisements, with only minimal information leaving the user's device and behavioural targeting taking place exclusively in the user's browser. In addition, the authors refer to Google's so-called *Federated Learning of Cohorts* (FLoC) system for microtargeting within Chrome.

reasonable expectations of the data subjects should also be taken into account in accordance with recital 47 of the GDPR, in addition to the special circumstances of the particular case²⁰⁶.

458. The criterion of the seriousness of the breach of the rights and freedoms of the data subject constitutes an essential element of the case-by-case assessment required by Article 6.1.f GDPR²⁰⁷. In this context, according to the Court of Justice, particular account should be taken of 'the nature of the personal data concerned, in particular their potentially sensitive nature, and of the nature and specific way in which they are processed, in particular the number of persons having access to them and the way in which they acquire such access'²⁰⁸.
459. Once again, the Litigation Chamber finds that due to the large number of TCF partners that may receive their personal data, data subjects cannot reasonably expect the processing associated with this disclosure. In addition, there is the considerable amount of data that, in accordance with the preferences entered within the TCF system, is collected by means of a *bid request* and transmitted to the adtech vendors within the context of the OpenRTB protocol²⁰⁹.
460. Furthermore, as the EDPB states, the legitimate interest does not constitute a sufficient legal basis in the context of direct marketing involving behavioural advertising²¹⁰. In addition, the ICO concluded in a recent report that the legitimate interest is not a basis for legality in the context of RTB (yet many publishers rely on this legal ground for their processing)²¹¹. In short, in view of the above, the Litigation Chamber has decided that the third condition imposed by Article 6.1.f GDPR and the case law of the Court of Justice has not been met *in this case*.
461. In light of the aforementioned considerations, the Litigation Chamber finds that **the legitimate interest of participating organizations cannot be deemed an adequate legal**

²⁰⁶ CJEU Judgment of 11 December 2019, *TK v. Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 58.

²⁰⁷ *Ibidem*, para. 56.

²⁰⁸ CJEU Judgment of 11 December 2019, *TK v. Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, para. 57.

²⁰⁹ Norsk Forbrukerrådet - "Out of Control. How consumers are exploited by the online advertising industry", 14 January 2020, <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/>, pp. 36-37; see also Recommendation CM/Rec(2021)8 of the Committee of Ministers of the Council of Europe to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 3 November 2021: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a46147>.

²¹⁰ Article 29 Working Party - Opinion 03/2013 on purpose limitation (WP 203), 2 April 2013, p. 46: "consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research".

²¹¹ Information Commissioner's Office - "Update report into adtech and real time bidding", 20 June 2019, <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>

ground for the processing activities occurring under the OpenRTB, based on users' preferences and choices captured under the TCF.

- (iii) - Contractual necessity is not a valid basis for the processing of personal data in the context of TCF and OpenRTB
462. In line with the EDPB guidelines, the Litigation Chamber notes that, in general, the (pre)contractual necessity of the processing is not a legal ground applicable to behavioural advertising²¹².
463. Moreover, the Litigation Chamber notes that the current version of the TCF does not mention Article 6.1.b GDPR anywhere as a possible legal basis for the processing of personal data within the TCF and OpenRTB.
464. **On the basis of the foregoing elements, the Litigation Chamber therefore concludes that the processing of personal data under the OpenRTB on the basis of preferences captured in accordance with the current version of the TCF is incompatible with the GDPR, due to an inherent breach of the principles of lawfulness and fairness.**

B.4.2. - Duty of transparency towards data subjects (Art. 12, 13 and 14 GDPR)

465. The complainants raise the issue of the lack of transparency, and more specifically the fact that the OpenRTB ecosystem is so extensive that it is impossible for data subjects to give an informed consent to the processing of their personal data, or to object in an informed manner to the processing of their personal data on the basis of a legitimate interest.
466. The defendant, on the other hand, states that the TCF offers a solution to collect valid consent from users, where applicable, in accordance with the requirements set out in the GDPR and the ePrivacy Directive²¹³.
467. The Litigation Chamber finds that the information provided under the TCF in its current format to data subjects, albeit for the purposes of processing their personal data in the context of OpenRTB, does not meet the transparency requirements under the GDPR²¹⁴.
468. First of all, the Litigation Chamber states that IAB Europe may in certain cases claim the "records of consent" that CMPs are required to keep, in accordance with the *TCF Policies*²¹⁵, but fails to inform data subjects of this possible processing by IAB Europe.

²¹² EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, v2.0, 8 October 2019, pp. 14 ff, <https://edpb.europa.eu>.

²¹³ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32); IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38).

²¹⁴ See para. 433 et seq. of this decision.

²¹⁵ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), pp. 11, 14 and 19.

469. Secondly, the Litigation Chamber finds that the manner in which information is provided to the data subjects, which was laid down by IAB Europe, does not comply with the requirement of a "transparent, comprehensible and easily accessible form"²¹⁶. The former Article 29 Working Party stipulates in its transparency guidelines that "the requirement that information and communication to data subjects be provided "in a concise, transparent, comprehensible and easily accessible form" means that data controllers should present the information/communication in an efficient and concise manner in order to avoid information fatigue"²¹⁷. Moreover, data subjects should be able to determine in advance the scope and consequences of the processing and not be surprised later by other ways in which their personal data have been used²¹⁸.
470. The Litigation Chamber finds that the approach taken so far does not meet the conditions of transparency and fairness required by the GDPR. Indeed, some of the stated processing purposes are expressed in too generic a manner for data subjects to be adequately informed about the exact scope and nature of the processing of their personal data²¹⁹. This is particularly problematic for purposes that rely on the consent of data subjects, as consent must be specific and sufficiently informed in order to be valid as a legal basis²²⁰.
471. The Litigation Chamber also refers to the examples of CMPs specified in the Technical Report of the Inspection Service, and notes that the interface offered to users does not allow, among other things, the processing purposes associated with the authorisation of a particular vendor or which adtech vendors will process their data for a specific purpose to be identified in a simple and clear manner²²¹.
472. In that regard, the Litigation Chamber emphasises that the large number of third parties, i.e. the *adtech vendors* that will potentially receive and process the personal data of the users contained in the bid request, based on the preferences they have submitted, is not compatible with the condition of a sufficiently informed consent, nor with the broader transparency duty set out in the GDPR.
473. On the basis of the foregoing elements, the Litigation Chamber must therefore rule that the TCF in its current set-up does not comply with the obligations arising from the transparency principle, notably Articles 12, 13 and 14 GDPR.

²¹⁶ Art. 12.1 GDPR.

²¹⁷ WP260 - Guidance on transparency under the GDPR, para. 8.

²¹⁸ WP260 - Guidance on transparency under the GDPR, para. 10.

²¹⁹ See para. 433 of this decision for examples as well as para. 441-452 for further analysis by the Litigation Chamber; see also C. MATT, C. SANTOS, N. BIELOVA, "Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?", in *Privacy Technologies and Policy*, APF 2020, LNCS, vol 12121, Springer, 2020, pp. 163-185.

²²⁰ See para. 429-440 of this decision.

²²¹ Technical Analysis Report of the Inspection Service, 6 January 2020 (Exhibit 53), pp. 99 et seq.

B.4.3. - Accountability (art. 24 GDPR), data protection by design and by default (Art. 25 GDPR), integrity and confidentiality (Art. 5.1.f GDPR), as well as security of processing (Art. 32 GDPR)

a. Principle of accountability and data protection by design and by default

474. Article 24.1 GDPR requires the data controller to implement appropriate technical and organisational measures, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Moreover, these measures shall be reviewed and updated as necessary. This article reflects the principle of “accountability” set out in Article 5.2 of the GDPR, according to which the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability). Article 24.2 of the GDPR stipulates that, where proportionate in relation to processing activities, the measures referred to in Article 24.1 GDPR shall include the implementation of appropriate data protection policies by the controller.
475. Recital 74 of the GDPR adds that “the responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. It is important, in particular, that the controller is responsible for implementing appropriate and effective measures and for demonstrating the conformity of the processing activities with this regulation, including the effectiveness of the measures. These measures must take account of the nature, scope, context and purpose of the trafficking and the risk it poses to the rights and freedoms of physical persons”.
476. It is also incumbent on the controller, pursuant to Articles 24 (accountability) and 25 of the GDPR (data protection by design and by default), to integrate the necessary respect for the GDPR rules into its processing and procedures, e.g. to ensure the existence and effectiveness of procedures for handling data subject requests and for checking the integrity and compliance of the TC String.

b. The outline of the security obligation

477. Pursuant to Article 32 of the GDPR, the controller is responsible for ensuring the security of the processing, “taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons”. In the present case, the Litigation Chamber notes a lack of respect for the obligation to ensure the security of processing on the part of the defendant, which is part of the principle of accountability. This shortcoming will be addressed *below*.

478. This failure to meet the obligation to ensure the security of processing constitutes a fundamental point of the present decision and of the penalties it imposes. The absence of technical and organisational measures aiming to ensure or tend to ensure the integrity of the TC String is considered a serious offence.
479. On the basis of Article 5.1.f GDPR, personal data must be processed in such a way as to ensure appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In the absence of appropriate measures to secure the personal data of the data subjects, the effectiveness of the respect of the fundamental rights to privacy and to the protection of personal data cannot be guaranteed, especially in view of the crucial role played by information and communication technologies in our society.
480. As indicated in the previous section, the lack of an obligation to ensure the security of processing constitutes an important point in the decision²²². Given the very large number of TC Strings generated each day within the TCF, it is essential that all the rules governing participation in the TCF are observed and complied with by all the parties involved, under the supervision of IAB Europe as the "*Managing Organisation*". The Litigation Chamber recalls that the combined reading of articles 32 (Security of processing), as well as 5.2 and 24 GDPR (principle of accountability) requires the controller to demonstrate its compliance with Article 32, by taking appropriate technical and organisational measures, in a transparent and traceable manner.
481. The Litigation Chamber also recalls the requirement of Article 25 GDPR (data protection by design and by default), which requires the data controller to integrate the necessary compliance with the rules of the GDPR upstream of its actions.
482. It should also be noted that the principle of security with its various components of integrity, confidentiality and availability of the data is set out in Articles 5.1.f and 32 of the GDPR and is now regulated in the GDPR at the same level as the fundamental principles of legality, transparency and loyalty.
483. IAB Europe offers the TCF to make OpenRTB compliant with the GDPR. In other words, the purpose of the TCF is to ensure that processing of personal data within the context of the OpenRTB protocol takes place in accordance with the GDPR as well as the ePrivacy Directive. Accordingly, IAB Europe, as *Managing Organisation* for the TCF and jointly responsible for the processing operations carried out within that framework²²³, should take

²²² See para. 478 et seq. of this decision.

²²³ See *supra*, title B.2. - Responsibility of IAB Europe for the processing operations within the Transparency and Consent Framework.

organisational and technical measures to ensure that participants at least comply with the TCF policies.

484. Notwithstanding the fact that in IAB Europe's current TCF system, *adtech vendors* receive consent signals as part of an HTTP(S) request or via browser APIs, some authors take the view that insufficient measures are in place under the TCF to guarantee the integrity of consent signals (particularly their validity) and to ensure that a *vendor* has actually received them (as opposed to having generated them itself)²²⁴.
485. However, in the absence of validation by IAB Europe, it becomes theoretically possible for CMPs to falsify or modify the signal to generate a *euconsent-v2* cookie and thus reproduce a "false consent" from users for all purposes and all *adtech vendors*. This case is also explicitly provided for in the TCF Policies:

*"A Vendor must not create Signals where no CMP has communicated a Signal and shall only transmit Signals communicated by a CMP or received from a Vendor who forwarded a Signal originating from a CMP without extension, modification, or supplementation, except as expressly allowed for in the Policies and/or Specifications."*²²⁵

486. The Litigation Chamber takes note of the fact that the possibility of falsification or modification of the TC String by CMPs is foreseen in the defendant's *Transparency & Consent Framework Policies* document, which sets out the basis for the TCF.
487. The Litigation Chamber also relies on the fact that the defendant indicates on its website the introduction of the "*TCF Vendor Compliance Programme*", through which audits of organisations participating in the TCF (listed on the *Global Vendors List*) will take place²²⁶. The Litigation Chamber encourages all initiatives on the part of the defendant, that are aimed at ensuring compliance with the obligation to process personal data under the TCF in a secure manner on the part of the defendant. Nevertheless, in view of the defendant's lack of systematic monitoring of compliance with the TCF rules by the participating organisations, and taking into account the significant impact of such violations (e.g. falsification or modification of the TC String), the Litigation Chamber considers that this initiative to introduce the TCF Vendor Compliance Programme is insufficient to bring the defendant into compliance with the security obligation.
488. In particular, the Litigation Chamber relies on the fact that the sanctions regime of this new programme, provided by the defendant in the case of failure to comply with the rules of the

²²⁴ See on this subject, for example C. SANTOS, M. NOUWENS, M. TOTH, N. BIELOVA, V. ROCA, "Consent Management Platforms Under the GDPR: Processors and/or Controllers?", in *Privacy Technologies and Policy*, APF 2021, LNCS, vol 12703, Springer, 2021, p. 64.

²²⁵ IAB Europe Transparency & Consent Framework Policies, Chapter III 13 (6), https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/#13_Working_with_CMPs

²²⁶ <https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/>

TCF, is permissive and not dissuasive. In fact, a vendor may declare himself liable for a breach up to 3 times, without any sanction, before being given 28 days to comply. Only in the event of non-compliance after the expiry of the 28 days will the vendor be removed from the *Global Vendors List*. It can also re-enter the list if it complies with the requirements later on. The programme also allows a vendor to be in breach up to four times, in order to proceed to an immediate suspension during a brief period of 14 days, until the vendor comes into compliance. The " *TCF Vendor Compliance Programme* " is therefore not a sufficient measure for ensuring the security of personal data processing operations carried out under the TCF.

489. The Litigation Chamber also observes that no measures other than the « TCF Vendor Compliance Programme » are foreseen by the defendant to monitor or prevent the falsification or modification of the TC String.
490. With regard to the allegation by the plaintiffs that IAB Europe also violates Articles 44 to 49 GDPR, the Litigation Chamber acknowledges, in view of the scope of the Framework – which involves a large number of participating organisations – that it is evident that personal data captured in the TC Strings will be transferred outside the EEA at some point by CMPs, and that the defendant is acting as data controller in this regard (see para. 356-357). However, the Litigation Chamber notes that the Inspection Service did not include an assessment of a concrete international data transfer in its report. For this reason, the Litigation Chamber concludes that there is an infringement of the GDPR, but in view of the lacking evidence of a systematic international transfer, as well as the scope and nature thereof, the Litigation Chamber finds it is not in a position to sanction the defendant for a violation of articles 44 to 49 GDPR. Notwithstanding the previous, the Litigation Chamber also finds that these international transfers of personal data, where applicable, must be assessed primarily by the publishers and CMPs implementing the TCF. The Litigation Chamber finds that the publishers are responsible and accountable for taking the necessary measures to prevent personal data collected through their website and/or application from being transferred outside the EEA without adequate international transfer mechanisms.
491. This being said, the Litigation Chamber also finds that the defendant should facilitate the due diligence incumbent on the publishers and CMPs, e.g. by requiring *adtech* vendors to indicate clearly whether they are located outside the EEA or whether they intend to transfer personal data outside the EEA through their data processors. Furthermore, the Litigation Chamber notes that, contrary to its obligation under the principles of accountability and of data protection by design and by default, IAB Europe did not foresee any mechanism to ensure that participating publishers and CMPs have put in place adequate mechanisms for potential international transfers of the TC String, as foreseen under Articles 44 to 49 GDPR, both at the time of its creation and when transmitting the TC String to participating *adtech* vendors. The preamble of the TCF Policies merely indicates that the TCF "is not

intended nor has it been designed to facilitate [...] more strictly regulated processing activities, such as transferring personal data outside of the EU". The Litigation Chamber finds that this does not meet the requirements of Articles 24 and 25 GDPR.

492. The Litigation Chamber notes, for the record, that it is uncertain whether, in view of its current architecture and support of the OpenRTB protocol, the TCF can be reconciled with the GDPR.
493. In this sense, IAB Europe's accountability starts from the moment the organisation designs and makes available a system for the management of consent or objections of users, but fails to take the necessary measures to ensure the conformity, integrity and validity of that consent or objection.
494. The Litigation Chamber therefore finds that, as part of its security and integrity obligations, IAB Europe must take not only organisational but also technically effective measures to ensure and demonstrate the integrity of the preferential signal transmitted by CMPs to *adtech vendors*.

B.4.4. - Additional alleged breaches of the GDPR

a. Purpose limitation and data minimisation (Art. 5.1.b and 5.1.c GDPR)

495. Although in this decision the Litigation Chamber has already concluded that the processing operations carried out on the basis of the OpenRTB protocol are not in accordance with the basic principles of purpose limitation and data minimisation²²⁷ (as no safeguards are provided to ensure that the personal data collected and disseminated within the framework of the OpenRTB are limited to information that is strictly necessary for the intended purposes), the Litigation Chamber emphasises that the complainants have explicitly indicated in their submissions that the scope of their allegations is limited to the processing operations within the TCF. The Inspection Service also clarified in its report that IAB Europe does not act as a data controller for the processing operations that take place entirely in the context of the OpenRTB protocol.
496. Taking these clarifications into account, the Litigation Chamber concludes that, given the limited amount of data about a user that is stored in a TC String before being saved by means of a *euconsent-v2* cookie, there is no violation of the principles of purpose limitation and data minimisation in the context of the TCF.

²²⁷ See para. 495-496 of this decision

497. Although larger quantities of personal data will be processed at a later stage, including special categories of personal data, this is not the case with the TCF. Within the TCF, therefore, there is no violation of the principles of purpose limitation and data minimisation.

b. Storage limitation (Art. 5.1.e GDPR)

498. With regard to the principle of storage limitation and based on the Inspection Service's report, the Litigation Chamber finds there is insufficient evidence that the TC String and the associated storage of users' personal data are stored for an unauthorised period of time, in violation of Article 5.1.e GDPR.

499. Therefore, the Litigation Chamber concludes that no violation of article 5.1.e GDPR could be established.

c. Integrity and confidentiality (Art. 5.1.f GDPR)

500. As already explained above²²⁸, the Litigation Chamber finds that the current version of the TCF offers insufficient safeguards to prevent the values included in a TC String from being modified in an unauthorised manner, with the result that the personal data of a data subject bundled in a *bid request* may be processed for the wrong purposes, in breach of the integrity principle, and/or may end up with the wrong *adtech vendors* or the ones rejected by the user, in breach of the confidentiality principle. The Litigation Chamber therefore rules that the current version of the TCF violates Article 5.1.f of the GDPR.

d. Processing of special categories of personal data (Art. 9 GDPR)

501. Although a number of complaints are directed against the RTB system, including the *Authorized Buyers* protocol developed by Google as well as the OpenRTB protocol developed by IAB Tech Lab, the Inspection Service determined in its report, as a preliminary matter, that the Belgian Data Protection Authority did not have jurisdiction for the former and that IAB Tech Lab does not act as a data controller for the latter²²⁹.

502. The Litigation Chamber notes that the Inspection Service reports the lack of appropriate rules for the processing of special categories of personal data under the TCF. However, this observation is not supported by any technical analysis showing that special categories of personal data are actually processed *within the TCF*. On the contrary, the technical analyses by the Inspection Service show that the TC String in itself does not contain any information that can be linked to the taxonomy of the websites visited, where, for example, special categories of personal data may be involved.

²²⁸ See para. 477 et seq. of this decision.

²²⁹ Investigation report of the Inspection Service, pp. 8-11.

503. Therefore, the Litigation Chamber rules that this allegation is unfounded and that no breach of Article 9 of the GDPR by the defendant can be established.

e. Exercise of data subject rights (Art. 15 – 22 GDPR)

504. First of all, the Inspection Service notes in its report that certain complainants have argued the impossibility for the data subjects to enforce their rights, although the investigation carried out by the Inspection Service did not confirm these allegations. In view of the lack of evidence of any infringement, the Litigation Chamber limits its reasoning to general observations relating to the exercise of data subject rights.

505. Secondly, the Litigation Chamber refers to the scope of the written submissions by the complainants, in which they specifically restricted their grievances to the processing of the plaintiffs' personal data by the defendant in the particular context of the TCF²³⁰. As a result, the Litigation Chamber will not assess the circumstances in which data subjects may exercise their rights regarding the processing of personal data contained in the *bid* requests, with respect to the adtech vendors, seeing as this processing occurs entirely under the OpenRTB protocol.

506. However, with regard to the current version of the TCF, the Litigation Chamber finds that the TCF does not seem to facilitate the exercise of the data subjects' rights insofar as the CMP interface cannot be retrieved easily and at all times by the users, such as to allow them to amend their preferences and retrieve the identity of the adtech vendors with whom their personal data have been shared by means of a bid request, in accordance with the OpenRTB protocol. In this regard, the Litigation Chamber underlines the importance of a proper implementation and enforcement of the interface requirements defined in the TCF Policies, such as to allow data subjects to effectively exercise their rights vis-à-vis each of the joint-controllers, and notes that the shared responsibility to do so lies primarily with the CMPs and publishers. In the light of the foregoing, the Litigation Chamber is, however, not in a position to establish a violation of the Articles 15-22 GDPR.

f. Records of processing activities (Art. 30 GDPR)

507. The Inspection Service notes in its report that IAB Europe does not keep records of its processing activities. The defendant takes the view, first of all, that it can rely on the exception provided for in Article 30.5 of the GDPR and is therefore not subject to the obligation to keep such records. However, in the course of the investigation, the defendant added a summary of its processing activities to the documents in the file²³¹.

²³⁰ Submission of the complainants dd. 18 February 2021, p. 2.

²³¹ IAB Europe's response to the investigation 10 February 2020 (Exhibit 57), p. 23.

508. The Litigation Chamber first notes that the records submitted by the defendant do not contain any activity relating to the TCF, with the exception of *member management*, *including administration of the TCF*. Contrary to the defendant's assertion, in particular that the records do not need to include the processing activities in the context of the TCF, the Litigation Chamber is of the opinion that the records must at least include access to users' consent signals, objections and preferences.
509. Indeed, in accordance with Article 8 of the *TCF Policies* (v1.1)²³² and Article 15 of the *TCF Policies* (v2.0)²³³, the defendant reserves the right, as the *Managing Organisation*, to access the "records of consent". The Litigation Chamber also emphasises that the incidental nature of this access to users' preferences has not been proven or raised by the defendant. The stable relationship between IAB Europe as *Managing Organisation* and all organisations participating in the TCF ecosystem should also be taken into account. In view of the large number of participating organisations and the defendant's intention to monitor the compliance of the various CMPs and other *adtech vendors*²³⁴, more thoroughly in the future, IAB Europe should also include this processing in its records of processing activities.
510. Therefore, the Litigation Chamber considers the non-incidental nature of the processing and the infringement of Article 30.1 GDPR found by the Inspection Service to be sufficiently proven.

g. Data protection impact assessment (Art. 35 GDPR)

511. The Litigation Chamber first notes that the defendant does not deny that the TCF can also be used for RTB purposes.
512. The argumentation by the defendant that the TCF can be used for other, non-marketing-related purposes and that the OpenRTB can also operate separately from the TCF is therefore not relevant to the consideration of whether or not a data protection impact assessment is required.
513. After all, the interrelationship between the TCF and the RTB implies that the preferences users enter by using a CMP interface will necessarily have an impact on the way their personal data are subsequently processed by adtech vendors within the RTB, as determined by the OpenRTB specification.

²³² IAB Europe Transparency & Consent Framework Policies v2019-04-02.2c (Exhibit 38), p. 6.

²³³ IAB Europe Transparency & Consent Framework Policies v2019-08-21.3 (Exhibit 32), p. 14.

²³⁴ Cf. Hearing of 11 June 2021.

514. The Litigation Chamber further refers to Decision No. 01/2019 of the General Secretariat of the Belgian DPA²³⁵, in which the General Secretariat has established a list of processing operations for which a data protection impact assessment is mandatory.
515. It is undisputed for the Litigation Chamber that the TCF was developed, among other things, for the RTB system, in which the online behaviour of users is observed, collected, recorded or influenced in a systematic and automated manner, including for advertising purposes²³⁶. It is also not disputed that within the RTB, data is widely collected from third parties (Data Management Platforms, or DMPs) in order to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons²³⁷.
516. Considering the large number of data subjects who come into contact with websites and applications implementing the TCF, as well as the growing number of organisations participating in the TCF, on the one hand, and the impact of the TCF on the large-scale processing of personal data in the context of RTB, on the other, the Litigation Chamber finds that, in accordance with Decision No. 01/2019, the Defendant is indeed subject to the obligation to conduct a data protection impact assessment, pursuant to Article 35 of the GDPR. Hence, Article 35 of the GDPR is violated.

h. Designation of a Data Protection Officer (art. 37 GDPR)

517. Article 37 GDPR provides for an obligation to designate a Data Protection Officer (DPO) in cases where:
- i. processing is carried out by a public authority or public body; or
 - ii. a controller or processor is primarily responsible for processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - iii. the controller or processor is primarily responsible for the processing of large volumes of special categories of personal data under Article 9 of the GDPR and of personal data relating to criminal convictions and offences under Article 10 of the GDPR.

²³⁵ Decision of the General Secretariat No. 01/2019 of 16 January 2019, available on the website of the GBA <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf>.

²³⁶ Decision of the General Secretariat No. 01/2019 of 16 January 2019, para. 6.8).

²³⁷ Decision of the General Secretariat No. 01/2019 of 16 January 2019, para. 6.3).

518. The Litigation Chamber has already concluded that the defendant processes personal data because IAB Europe, in its capacity as *Managing Organisation*, can have access to the TC Strings and *the records of consent*²³⁸.
519. The former Article 29 Working Party states that processing activities that are necessary to achieve the purposes of the controller or processor can be considered as core activities within the meaning of Article 37 GDPR. The Litigation Chamber finds that in view of the importance of the TCF to the defendant, the stated purposes of the TCF, as well as the associated processing of personal data in its capacity as *Managing Organisation*, the processing under the TCF belongs to the core activities of IAB Europe.
520. With regard to the concept of 'large-scale processing operations', the Article 29 Working Party clarifies that, *inter alia*, the following must be taken into account:

- i. the number of data subjects - either as a specific number or as a proportion of the relevant population;
- ii. the amount of data and/or range of the different data items processed;
- iii. the duration or permanence of data processing;
- iv. the geographical extent of the processing activity.

In the present case, the Litigation Chamber finds that the TCF is offered in various Member States; that the TCF intrinsically requires that the personal data of users be processed in the form of a TC String for as long as this is necessary to be able to demonstrate that consent was obtained in accordance with the *TCF Policies*; and that the personal data processed is furthermore shared with numerous *adtech vendors*. From this, the Litigation Chamber concludes that the TCF involves the large-scale processing of personal data.

521. With regard to the criterion of regular and systematic observation the WP29 interprets the term "regular" in one or more of the following ways:
- i. something that occurs continuously or at specific times during a certain period of time
 - ii. something that occurs in a recurring manner, or repetitively at fixed times; or
 - iii. something that occurs constantly or periodically

The Litigation Chamber finds that the contractual obligation for *Vendors* and *CMPs* to submit records of consent to the defendant, in its capacity as *Managing Organisation*, upon simple request by IAB Europe falls within (i). Thus, there is regular observation of data relating to identifiable users.

522. The term "systematic" should be understood in one or more of the following ways:

²³⁸ See para. 358 and 468 of this decision.

- i. Something that occurs according to a system
 - ii. Prearranged, organised or methodical
 - iii. Something that occurs in the context of a general data collection programme
 - iv. Something carried out as part of a strategy
523. Once again, the Litigation Chamber finds that the processing of the TC Strings or *records of consent* by the defendant in the current version of the TCF meets at least the first three criteria. Therefore, the Litigation Chamber rules that the TCF must be regarded as a regular and systematic observation of identifiable users.
524. From the foregoing elements, the Litigation Chamber concludes that IAB Europe should have appointed a DPO, in accordance with Article 37 GDPR. Hence, Article 37 of the GDPR is violated.

C. Sanctions

525. As a preliminary matter, and as developed below, the Litigation Chamber notes that the present decision on the TCF does not directly address deficiencies of the wider OpenRTB framework. However, the Litigation Chamber does draw attention to the great risks to the fundamental rights and freedoms of the data subjects posed by OpenRTB, in particular in view of the large scale of personal data involved, the profiling activities, the prediction of behaviour, and the ensuing surveillance (see A.3.1. **- Definitions and operation of the Real-Time Bidding system**). Insofar as the TCF is the tool on which OpenRTB relies to justify its compliance with the GDPR, the TC String plays a pivotal role in the current architecture of the OpenRTB system.

526. Under Article 100 of the DPA Act, the Litigation Chamber has the power to:
- 1° classify the complaint without taking action;
 - 2° order the dismissal of the case;
 - 3° pronounce a suspension of the pronouncement;
 - 4° propose a transaction;
 - 5° formulate warnings or recommendations;
 - 6° order to comply with the requests of the person concerned to exercise these rights;
 - 7° order that the interested party be informed of the security problem;
 - 8° order the freezing, restriction or temporary or permanent prohibition of processing;
 - 9° order the compliance of the treatment;
 - 10° order the rectification, restriction or erasure of data and the notification to recipients of the personal data;

- 11° order the withdrawal of the certification bodies' accreditation;
- 12° impose fines;
- 13° impose administrative fines;
- 14° order the suspension of data flows to another State or international body;
- 15° forward the file to the Brussels Public Prosecutor's Office, which informs it of the action relating to the file;
- 16° decide, case by case, to publish its decisions on the internet site of the Data Protection Authority.

527. As for the administrative fine that may be imposed pursuant to Article 83 of the GDPR and Articles 100, 13° and 101 DPA Act, Article 83 of the GDPR provides:

« 1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

- a) *the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
- b) *the fact that the violation has been committed deliberately or through negligence;*
- c) *any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
- d) *the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
- e) *any relevant previous infringements by the controller or processor;*
- f) *the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
- g) *the categories of personal data affected by the infringement;*
- h) *the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
- i) *where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*
- j) *adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. ».

528. Recital 150 GDPR²³⁹ further distinguishes between whether the offender is an undertaking or not. In the first hypothesis, the criterion (fixed amount or percentage) for reaching the highest fine should be applied. Where, on the other hand, the offender is not an undertaking, account should be taken of the economic situation of the offender and the general level of incomes in the Member State concerned. This is to prevent the imposition of fines that could be disproportionately high.
529. It is important to contextualise the shortcomings of the defendant in order to identify the most appropriate corrective measures. In this context, the Litigation Chamber will take into account all the circumstances of the case, including – within the limits it specifies below – the reaction submitted by the defendant to the envisaged sanctions communicated by means of the sanction form²⁴⁰. In this regard, the Litigation Chamber specifies that the form it sent expressly mentions that it does not involve the reopening of debates. Its sole purpose is to collect the defendant's reaction to the planned sanctions.
530. While measures such as a compliance order or a ban on further processing can put an end to an identified infringement, administrative fines, as set out in Recital 148 of the GDPR, are imposed in case of serious infringements, in addition to or instead of the appropriate measures that are required to remedy the infringement.
531. The Litigation Chamber would also like to point out that it is its sovereign responsibility as an independent administrative authority – in compliance with the relevant articles of the GDPR and the DPA Act – to determine the appropriate corrective measure(s) and sanction(s). This follows from Article 83 GDPR itself, but also the Market Court has emphasised the existence of a wide margin of manoeuvre in its case law, *inter alia* in its judgment of 7 July 2021²⁴¹.
532. The Litigation Chamber notes that the complainants are making various requests for sanctions against the defendant. However, it is not for the complainants to ask the Litigation Chamber to order any particular corrective measure or sanction, nor is it up to the Litigation Chamber to give reasons for not accepting any of the requests made by the

²³⁹ Recital 150 of the GDPR: [...] Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine.[...].

²⁴⁰ See para. 534 as well as para. 272 *et seq.* of this decision.

²⁴¹ Court of Appeal of Brussels, Market Court Section, 19th Chamber A, Market Cases Section, 2021/AR/320, pp. 37-47.

complainants²⁴². These considerations nevertheless leave intact the obligation for the Litigation Chamber to give reasons for the choice of measures and sanctions which it deems appropriate (from the list of measures and sanctions made available to it by Article 58 of the GDPR and Article 100 of the DPA Act) to sentence the defendant.

533. In the present case, the Litigation Chamber notes that the complainants request the Litigation Chamber to take the following measures and sanctions. These proposals are included for information:

"1) *In application of Article 100, §1, 8° DPA Act (relating to IAB Europe) to:*

- a. *prohibit the TC String to be processed in the TCF;*
- b. *prohibit all personal data associated with the processing of the TC String, such as IP addresses, websites visited and apps used, from being processed in the TCF;*
- c. *order the permanent removal from its website and its other public communication channels of all documents, files and records that in any way incite or oblige any third party to carry out such processing;*

2) *In application of Article 100, §1, 10° DPA, order IAB Europe to permanently delete all TC Strings and other personal data already processed in the TCF from all its IT systems, files and data carriers, and from the IT systems, files and data carriers of processors contracted by IAB Europe;*

3) *In application of Article 100, §1, 10° DPA Act order IAB Europe to inform all recipients of the personal data processed in the TCF of the order imposed by the Litigation Chamber:*

- a. *prohibition to process the TC String in the TCF;*
- b. *prohibit all personal data associated with the processing of the TC String, such as IP addresses, websites visited and apps used, from being processed in the TCF;*
- c. *order to permanently delete all TC Strings and other personal data already processed in the TCF from all IT systems, files and data carriers;*

and this both clearly visible and readable in a bold box at the top of the homepage of IAB Europe's website www.iabeurope.eu in the usual font and size until 6 months after a judgment of the Market Court becomes final, if applicable pursuant to Section 108 of the DPA Act, or by email, in both cases with a hyperlink to the English-language version of the decision of the Litigation Chamber on the website of the GBA;

4) *In application of Article 100, §1, 12° DPA Act on behalf of IAB Europe order the forfeiture of a penalty payment of EUR 25,000 per started calendar day of delay in the execution of any measure imposed in the interlocutory decision of the Litigation Chamber as from the expiration of seven calendar days after the interlocutory decision of the Litigation Chamber."*

²⁴² See Court of Appeal of Brussels, Market Court Section, 19th Chamber A, Market Cases Section, 1 December 2021, 2021/AR/1044, p. 25.

534. A sanction form has been sent to the defendant on 11 October 2021. IAB Europe submitted its response on 1 November 2021²⁴³. This response has been taken into consideration in the following paragraphs.

C.1. - Breaches

535. The Litigation Chamber found the defendant in breach of the following articles:

- **Articles 5.1.a and 6 GDPR** — The current TCF does not provide a legal basis for the processing of user preferences in the form of a TC String. Moreover, the Litigation Chamber notes that the TCF offers two bases for the processing of personal data by participating adtech vendors, but finds that none of them can be used. First, the consent of the data subjects is currently not given in a sufficiently specific, informed and granular manner. Second, the legitimate interest of the organisations participating in the TCF is outweighed by the interests of the data subjects, in view of the large-scale processing of the users' preferences (collected under the TCF) in the context of the OpenRTB protocol and the impact this can have on them. Since none of the grounds for lawfulness set out in Article 6 of the GDPR apply to this processing, as explained above²⁴⁴, the defendant is in breach of Articles 5.1.a and 6 GDPR.

Taking note of the fact that the defendant itself does no longer have factual or technical control over the TC Strings once these have been generated by the CMPs and stored on the users' devices²⁴⁵, the Litigation Chamber finds that it cannot impose the *a posteriori* removal of all TC Strings generated until now on the defendant. More specifically, it is the responsibility of the CMPs and the publishers who implement the TCF²⁴⁶, to take the appropriate measures, in line with Articles 24 and 25 GDPR, ensuring that personal data that has been collected in breach of Articles 5 and 6 GDPR is no longer processed and removed accordingly. Insofar as IAB Europe is still storing TC Strings deriving from the no longer supported globally scoped consent cookies, the Litigation Chamber equally finds that the necessary measures must be taken by the defendant to warrant permanent erasure of these no longer necessary personal data.

- **Articles 12, 13, and 14 GDPR** — As developed above (see *B.4.2. - Duty of transparency towards data subjects (Art. 12, 13 and 14 GDPR)*), the way in which the information is provided to the data subjects does not meet the requirement of a 'transparent, comprehensible and easily accessible manner'. Users of a website or an application

²⁴³ See title A.10. - Sanction form, European cooperation procedure, *supra*.

²⁴⁴ See title B.4.1 - Lawfulness and fairness of processing (Art. 5.1.a and 6 GDPR).

²⁴⁵ In accordance with the mandatory policies and technical specifications established and imposed on TCF participants by IAB Europe.

²⁴⁶ Furthermore, the Litigation Chamber underlines the fact that none of the CMPs and adtech vendors haven taken part in the present proceedings.

participating in the TCF are not given sufficient information about the categories of personal data collected about them, nor are they able to determine in advance the scope and consequences of the processing. The information given to users is too general to reflect the specific processing of each vendor, which also prevents the granularity — and therefore the validity — of the consent received for the processing carried out using the OpenRTB protocol. Data subjects are unable to determine the scope and consequences of the processing in advance, and therefore do not have sufficient control over the processing of their data to avoid being surprised later by further processing of their personal data.

- **Articles 24, 25, 5.1.f and 32 GDPR** — As explained above²⁴⁷, on the basis of Articles 5.1.f and 32 GDPR, the controller is obliged to ensure the security of the processing and the integrity of the personal data processed. The Litigation Chamber recalls that the combined reading of Articles 5.1.f and 32, as well as 5.2 and 24 GDPR (subjecting the controller to the principle of accountability) requires the controller to demonstrate its compliance with Article 32, by taking appropriate technical and organisational measures, in a transparent and traceable manner. Under the current TCF system, adtech vendors receive a consent signal without any technical or organisational measure to ensure that this consent signal is valid or that a vendor has actually received it (rather than generated it). In the absence of systematic and automated monitoring systems of the participating CMPs and *adtech vendors* by the defendant, the integrity of the TC String is not sufficiently ensured, since it is possible for the CMPs to falsify the signal in order to generate an *euconsent-v2* cookie and thus reproduce a "false consent" of the users for all purposes and for all types of partners. As indicated above²⁴⁸, this hypothesis is also specifically foreseen in the terms and conditions of the TCF. The Litigation Chamber therefore finds that IAB Europe, in its capacity of *Managing Organisation*, has designed and provides a consent management system, but does not take the necessary steps to ensure the validity, integrity and compliance of users' preferences and consent.

The Litigation Chamber also finds that the current version of the TCF does not facilitate the exercise of the data subject rights, especially taking into consideration the joint-controllership relation between the publisher, the implemented CMP and the defendant. The Litigation Chamber also underlines that the GDPR requires that data subjects rights can be exercised vis-à-vis each of the joint-controllers in the TCF such as to comply with Articles 24 and 25 GDPR.

²⁴⁷ See title B.4.3. - Accountability (art. 24 GDPR), data protection by design and by default (Art. 25 GDPR), integrity and confidentiality (Art. 5.1.f GDPR), as well as security of processing (Art. 32 GDPR)

²⁴⁸ See para. 485 of this decision.

In light of the above, the Litigation Chamber finds that the defendant is in breach of its obligations of security of processing, integrity of personal data, and data protection by design and data protection by default (Articles 24, 25, 5.1.f and 32 GDPR).

- **Article 30 GDPR** — As developed above²⁴⁹, the Litigation Chamber cannot follow the defendant's argument that it can benefit from the exceptions to the obligation to maintain records of processing activities, provided for in Article 30.5 GDPR. As the records of processing activities of the defendant do not contain any processing operations relating to the TCF, except for the management of members and the administration of the TCF, although IAB Europe as *Managing Organisation* can access the records of consent, the Litigation Chamber finds a breach of Article 30 GDPR by the defendant.
- **Article 35 GDPR** — In view of the large number of data subjects that come into contact with websites and applications implementing the TCF, as well as organisations participating in the TCF, on the one hand, and the impact of the TCF on the large-scale processing of personal data in the OpenRTB system, on the other hand, the Litigation Chamber finds that IAB Europe has failed to carry out a comprehensive data protection impact assessment (DPIA) with regard to the processing of personal data within the TCF, and thus violated Article 35 GDPR. The Litigation Chamber finds that the TCF was developed, among other things, for the RTB system, in which the online behaviour of users is observed, collected, recorded or influenced in a systematic and automated manner, including for advertising purposes. It is also not disputed that within the OpenRTB, data are widely collected from third parties (DMPs) in order to analyse or predict the economic situation, health, personal preferences or interests, reliability or behaviour, location or movements of natural persons.
- **Article 37 GDPR** — Because of the large-scale, regular and systematic observation of identifiable users that the TCF implies, and in view of the defendant's role, more specifically of its capacity as *Managing Organisation*, the Litigation Chamber rules that IAB Europe should have appointed a Data Protection Officer (DPO). By failing to do so, the defendant infringes Article 37 GDPR.

²⁴⁹ See para. 507 et seq. of this decision.

C.2. - Sanctions

536. Therefore, the Litigation Chamber orders the defendant:

- I. To render the TCF compliant with the obligation of lawfulness, fairness and transparency (Articles 5.1.a and 6 GDPR), by establishing a legal basis for the processing as well as the sharing of user preferences in the context of the TCF, in the form of a TC String and euconsent-v2 cookie placed on the users' devices for this purpose. These obligations also imply that any personal data collected so far by means of a TC String in the context of the globally scoped consents, which is no longer supported by IAB Europe, shall be deleted without undue delay by the defendant. In addition, the Litigation Chamber orders the defendant to prohibit the use of legitimate interest as a legal ground for processing by the organisations participating in TCF in its current format, via its terms of use.
- II. To render the TCF compliant with the transparency and information obligation (Articles 12, 13, and 14 of the GDPR), by requiring TCF-registered CMPs to take a harmonised and GDPR-compliant approach regarding the information to be provided to users through their interface. The information, which covers the categories of data collected, the purposes for which they are collected, and the applicable legal grounds for processing, must be precise, concise and understandable in order to avoid users being surprised by subsequent processing of their personal data by parties other than the publishers or IAB Europe.
- III. To ensure compliance of the TCF with the obligations of integrity and security, as well as data protection by design and by default (under Articles 5.1.f and 32 GDPR, and 25 GDPR). In this respect, the Litigation Chamber orders to include effective technical and organisational monitoring measures to facilitate the exercise of data subject rights and to guarantee the integrity of the TC String in view of the possibility, in the current state of the system, of falsification of the signal. An example of measures to be put in place under Article 32 of the GDPR is a strict vetting process for organisations participating to the TCF. The Litigation Chamber reminds the defendant as well as the other joint-controllers of their obligation to make the necessary arrangements such as to ensure, amongst other requirements, that data subjects may effectively exercise their rights. Lastly, in the context of Article 25 of the GDPR, the defendant must prohibit, via its terms of use, the organisations participating in the current version of TCF from activating a default consent, as well as from basing the lawfulness of the intended processing activities on the legitimate interest.
- IV. To ensure the compliance of the records of processing activities carried out in the framework of the TCF in its current format, and in particular relating to the

processing of users' preferences and consent in the form of a TC String and the placement of a cookie *euconsent-v2* on their devices.

- V. To carry out a data protection impact assessment, covering both the processing activities under the TCF and the impact of these activities on subsequent processing under the OpenRTB.
- VI. To designate a Data Protection Officer (DPO), responsible, *inter alia*, for ensuring the compliance of personal data processing activities in the context of the TCF, in accordance with Articles 37 to 39 of the GDPR.

537. These compliance measures should be completed within a maximum period of six months following the validation of an action plan by the Belgian Data Protection Authority, which shall be submitted to the Litigation Chamber within two months after this decision. On the ground of Article 100 § 1^{er}, 12° of the DPA Act, a penalty payment of 5.000 EUR per day will be due in case of failure to comply within the above-mentioned time limits.

538. In addition to this compliance order, the Litigation Chamber is of the opinion that an administrative fine is justified in this case for the following reasons, which are analysed on the basis of article 83.2 GDPR.

539. The principles of lawfulness, fairness, transparency and security are part of the essence of the GDPR and infringements of these rights are punishable by the highest fines, according to Article 83.5 GDPR. In this respect, the failure to respect the basic principles of data protection should be penalised by proportionately high fines, depending on the circumstances of the case. In this regard, reference can be made to the Guidelines on the Application and Setting of Administrative Fines, according to which:

« Fines are an important tool that supervisory authorities should use in appropriate circumstances. The supervisory authorities are encouraged to use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive as well as a proportionate reaction to the breach. The point is to not qualify the fines as last resort, nor to shy away from issuing fines, but on the other hand not to use them in such a way which would devalue their effectiveness as a tool. »²⁵⁰

540. In its subparagraph (a), article 83.2. refers to « the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them ».

541. With regard to the nature and gravity of the infringements, the Litigation Chamber notes that the principles of lawfulness (Articles 5.1.a and 6 GDPR), transparency (Articles 12 to 14

²⁵⁰ Article 29 Working Party – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253), p. 7.

GDPR) as well as security (Articles 5.1.f and 32 GDPR) are fundamental principles of the protection regime set up by the GDPR. The principle of accountability set out in Article 5.2. of the GDPR and developed in Article 24 is also at the heart of the GDPR and reflects the paradigm shift brought about by the GDPR, *i.e.* a shift from a regime based on prior declarations and authorisations by the supervisory authority to greater accountability and responsibility of the controller. Respect of its obligations by the latter and its ability to demonstrate this are therefore only more important.

542. A valid legal basis and transparent information are core elements of the fundamental right to data protection. As far as transparency is concerned, this principle is the 'gateway' that strengthens the control of data subjects over their personal data and enables the exercise of other rights granted to the data subjects by the GDPR, such as the right to object and the right of erasure. Breaches of these principles constitute serious infringements, which may be subject to the highest administrative fines foreseen under the GDPR.
543. The breach of Article 25, on the obligation of data protection by design and by default, as well as of Article 30 on keeping records of processing activities are also significant infringements, particularly in view of the scale of the processing operations and the impact on the privacy of the complainants as well as the other users confronted with websites or applications that have implemented the TCF.
544. As regards the nature and purpose of the processing, and more specifically on the nature of the data, the Litigation Chamber notes that the TC String, as an expression of users' preferences on the processing purposes and the potential adtech vendors being provided through the CMP interface, constitutes the cornerstone of the TCF. Although the scope of this decision is the TCF and its TC String, and the sanction imposed on the defendant pertains solely to that framework, the compliance of the OpenRTB with the GDPR is assessed as part of a holistic analysis of the TCF and its interaction with the former. Insofar as the current version of the TCF is the tool on which OpenRTB relies to justify its compliance with the GDPR, and because the defendant facilitates membership and use of the OpenRTB to a significant number of participating organisations, the Litigation Chamber finds that IAB Europe plays a pivotal role as regards the OpenRTB, without being a data controller in that context.
545. As regards the scope of the contested processing and the number of data subjects affected, the Litigation Chamber notes that the TCF (in its current format), as developed by the defendant (representing large players in the online behavioural advertising sector²⁵¹), offers a unique service on the market. The TCF's scope is therefore essential, given the growing number of partners that signed up to it. Regarding the level of damage incurred by

²⁵¹ See para. 36 of this decision.

concerned data subjects, the Litigation Chamber underlines once more that the TC String plays a pivotal role in the current architecture of the OpenRTB system. Thereby, the TC String supports a system posing great risks to the fundamental rights and freedoms of the data subjects, in particular in view of the large scale of personal data involved, the profiling activities, the prediction of behaviour, and the ensuing surveillance of data subjects.

546. With respect to the duration of the infringement, the Litigation Chamber takes note that the TCF is offered by the defendant since 25 April 2018 as a mechanism for obtaining users' consent with respect to predetermined processing purposes, and for the transfer of their personal data to TCF-participants, including adtech vendors. Notwithstanding the various iterations of the framework, which has been upgraded to the second version of the TCF on 21 August 2019, and taking into account the systemic deficiencies of the TCF under the GDPR, the Litigation Chamber finds that the breaches have existed at least since May 2018, with regard to the validity of the collected consent and the placement of a TC String without a valid legal ground, and since August 2019 for the reliance on legitimate interest as a legal ground to process the data subjects' personal data.
547. Article 83.2.b GDPR requires the DPA to take into account the intentional or negligent character of the infringement. Observing that the defendant, in its role as *Managing Organisation*, was aware²⁵² of risks linked to non-compliance with the TCF, in particular relating to the integrity of the TC String and the encapsulated choices and preferences of the users, and in light of the impact of the TC String on the subsequent processing operations under the OpenRTB, the Litigation Chamber finds that IAB Europe was negligent in establishing the measures governing the implementation of the current version of the TCF.
548. In its subparagraph (c), article 83.2 GDPR refers to potential actions taken by the controller to mitigate the damage suffered by data subjects. The Litigation Chamber notes the absence of concrete measures taken or introduced by the defendant in order to mitigate the damage suffered by the data subjects (i.e. the processing of their personal data regardless of their choices, or in the absence of a valid legal ground).
549. Article 83.2.d of the GDPR concerns the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32.
550. Even if the Litigation Chamber does not take into account in the present decision the developments that occurred after the closure of the proceedings in June 2021, the

²⁵² See para. 485 of this decision.

Litigation Chamber takes note that the defendant already announced during the hearing²⁵³ its intention to introduce a "TCF Vendor Compliance Programme" in September 2021, through which audits of organisations participating in the TCF (listed on the Global Vendors List) will be established.

551. The Litigation Chamber encourages all measures aimed at ensuring compliance with the GDPR. Nevertheless, as explained in para. 487-488, in view of the defendant's lack of systematic monitoring of compliance with the TCF rules by the participating organisations at the time of the complaints, and taking into account the significant impact of such violations (e.g. in case of falsification or modification of the TC String), the Litigation Chamber considers that the announcement of this initiative to increase its compliance with one of its obligations as a data controller for the TCF and consisting of audits of adtech vendors on the *Global Vendors List* demonstrates that the TCF was not compliant with the defendant's safety obligations, including the obligation to mitigate damage suffered by data subjects. No other actions were communicated by the defendant to the Litigation Chamber in this respect.
552. Furthermore, the Litigation Chamber is no longer in a position to review the nature of this programme and, in any event, this new programme does not change the nature of the breaches of the GDPR that occurred until the closure of the debates in June 2021.
553. In light of article 83.2.e of the GDPR, the Litigation Chamber notes the absence, at the time of the present decision, of any final decision by other competent supervisory authorities, regarding previous relevant infringements by the defendant in relation to the TCF.
554. Article 83.2.f of the GDPR concerns the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement. In this regard, the Litigation Chamber disagrees with the Inspection Service's finding that the defendant did not cooperate sufficiently with the former, apart from the provision and submission of records of processing activities conducted by IAB Europe.
555. Insofar as the categories of personal data affected by the infringement are concerned (Article 83.2.g of the GDPR), the Litigation Chamber acknowledges that the personal data contained in and processed by means of the TC String are in adequacy with the principle of data minimisation, having regard to their nature. Notwithstanding the previous, the Litigation Chamber reiterates its position that the TCF plays a pivotal role in supporting the processing operations based on the OpenRTB protocol. Hence, the Litigation Chamber concludes that it cannot exclude that both special and regular categories of personal data

²⁵³ And confirmed by the defendant through a public announcement on its website, on 26 August 2021: <https://iabeurope.eu/blog/iab-europe-launches-new-tcf-vendor-compliance-programme/>

—processed by means of a bid request to which the TC String is attached— may be affected by the infringements that occurred under the TCF.

556. With regard to article 83.2.h of the GDPR, the Litigation Chamber notes that this criterion is not relevant to the present case.
557. Article 83.2.i of the GDPR is not applicable in the absence of any previous final decision in this regard, taken against the defendant.
558. Article 83.2.j of the GDPR concerns the adherence to approved codes of conduct or approved certification mechanisms. In this context, the Litigation Chamber notes that IAB Europe has previously been in contact with the Belgian Data Protection Authority concerning the drafting and adoption of a Code of Conduct (at the point of time when the proceedings were already pending). The Litigation Chamber also underlines the absence of follow-up by the defendant in this regard since June 2020, without any further explanation by the defendant.
559. Lastly, article 83.2.k of the GDPR refers to any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. The Litigation Chamber did not retain specific factors that would change the amount of the fine.
560. In determining the amount of the administrative fine, article 83.3 to 83.7 GDPR use the term “undertaking”, which, based on Recital 150 of the GDPR and as confirmed by the WP29 and the EDPB²⁵⁴, should be understood in accordance with articles 101 and 102 TFEU. Based on CJEU case law, the term undertaking in Articles 101 and 102 TFEU refers to a single economic unit (SEU), even if this economic unit is legally formed from several natural or legal persons²⁵⁵.
561. To assess whether several entities form a SEU, the ability of the individual entity to take free decisions should be taken into account. It should also be considered whether a leading entity (the parent company), exercises decisive influence over the other entity or not (examples of criteria are the amount of the participation, personnel or organizational ties, instructions and the existence of company contracts).
562. The Litigation Chamber could not find any indication of decisive influence from IAB Inc. over the defendant IAB Europe, or limitation of freedom of its decision with respect to IAB Inc.

²⁵⁴ Article-29-Working Party – Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) and confirmed by the EDPB in Endorsement 1/2018 on 25 May 2018; as well as EDPB Binding Decision 1/2021, para. 292.

²⁵⁵ CJUE Judgment of 23 April 1991. *Klaus Höfner and Fritz Elser v Macrotron GmbH*, C-41/90, ECLI:EU:C:1991:161, paragraph 21, and CJUE Judgment of 14 December 2006, *Confederación Española de Empresarios de Estaciones de Servicio*, C-217/05, ECLI:EU:C:2006:784, para. 40

563. This was also developed by the defendant in its response to the sanction form, wherein IAB Europe claims that IAB Inc. has no ownership stake in the defendant nor any say in the deployment of IAB Europe's activities. The defendant indicated that IAB Inc. (headquartered in the USA) licenses the "IAB" brand to other organizations, and remains an entirely separate and independent entity from IAB Europe.
564. The Litigation Chamber therefore decides to base its decision on the sole financial revenues of IAB Europe as reference for calculating the administrative fine, instead of the annual turnover of IAB Inc.
565. In this regard, the Litigation Chamber takes note that the annual gross benefits of the defendant amounted to EUR 2.471.467 in 2020²⁵⁶. As a subsidiary point, the Litigation Chamber also observes that participating organisations are required to pay an annual fee of 1.200 EUR to the defendant upon their registration to the TCF²⁵⁷. Having regard to the total number of registered TCF adtech vendors, which has significantly increased from 420 on 25 May 2020 to 744 on 7 June 2021, the Litigation Chamber thus finds that a large part of the income of IAB Europe is generated through the licensing of the TCF. More specifically, IAB Europe would make a gross profit of at least 981.600 EUR for 2021 with the TCF participants' annual fee – including both the adtech vendors and the CMPs²⁵⁸ – alone.
566. Under Article 83.4, infringements of articles 25, 30, 32, 35 and 37 GDPR may amount to up to 10.000.000 EUR or, in the case of an undertaking, up to 2% of the total annual worldwide turnover of the preceding business year.
567. Under 83.5 GDPR, infringements of articles 5.1.a, 5.1.f, 6, and 12 to 14 GDPR may amount to up to 20.000.000 EUR or, in the case of an undertaking, up to 4% of the total annual worldwide turnover of the preceding business year. The maximum amount of the fine in this case, as provided for in Article 83.5, is therefore 20.000.000 EUR.
568. As these are, among other things, infringements of a fundamental right enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, the assessment of their seriousness based on Article 83.2.a GDPR will be made in an autonomous manner.
569. Based on the elements developed above, the defendant's reaction to the proposed sanction form, as well as the criteria listed in Article 83.2 GDPR, the Litigation Chamber considers that the above-mentioned infringements justify to impose a compliance order in conjunction with an administrative fine of 250.000 EUR (Article 100, § 1^{er}, 13° and 101 DPA Act) on the defendant, as an effective, proportionate and dissuasive sanction in light of

²⁵⁶ See Annual Accounts 21/12/2020, available at <https://cri.nbb.be/bc9/web/catalog?execution=e1s1>.

²⁵⁷ https://iabeurope.eu/wp-content/uploads/2019/08/TCF-Fact-Sheet_General.pdf

²⁵⁸ Totalling 74 CMPs on June 7th, 2021: <https://iabeurope.eu/cmp-list/>. The actual profit is likely to be higher, considering the still increasing number of TCF participants.

Article 83 GDPR. In fixing this amount, the Litigation Chamber took into account the annual business volume of the defendant, which amounted to 2.471.467 EUR in 2020²⁵⁹.

570. The amount of EUR 250.000 EUR remains, in view of the aforementioned elements, proportionate to the infringements that have been established by the Litigation Chamber. This amount is also much lower than the maximum amount of 20.000.000 EUR provided for by Article 83.5 GDPR.
571. The Litigation Chamber is of the opinion that a lower fine would not meet, in the present case, the criteria required by Article 83.1 of the GDPR, according to which the administrative fine must not only be proportionate, but also effective and dissuasive. These elements derive from the principle of loyal cooperation described in Recital 13 GDPR (in line with Article 4.3 of the Treaty on the European Union).
572. In view of the importance of transparency regarding the decision-making process of the Litigation Chamber and in accordance with Article 100, §1, 16° of the DPA Act, this decision is published on the website of the Data Protection Authority²⁶⁰. Having regard to the previous publicity surrounding this case, as well as the general interest to the public, also in view of the a large number of data subjects and organisations involved, the Litigation Chamber has decided not to delete the direct identification data of the parties and persons mentioned, whether natural or legal persons.

²⁵⁹ See Annual Accounts 21/12/2020 available at <https://cri.nbb.be/bc9/web/catalog?execution=e1s1>

²⁶⁰ See also para. 287.

FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation, to:

- order the defendant, pursuant to Article 100(1)(9) of the DPA Act, with a view to bring the processing of personal data within the context of the TCF in line with the provisions of the GDPR, by:
 - a. providing a valid legal basis for the processing and dissemination of users' preferences within the context of the TCF, in the form of a TC String and a *euconsent-v2* cookie, as well as prohibiting, via the terms of use of the TCF, the reliance on legitimate interests as a legal ground for the processing of personal data by organisations participating in the TCF in its current form, pursuant to Articles 5.1.a and 6 of the GDPR;
 - b. ensuring effective technical and organisational monitoring measures in order to guarantee the integrity and confidentiality of the TC String, in accordance with Articles 5.1.f, 24, 25 and 32 of the GDPR;
 - c. maintaining a strict audit of organisations that join the TCF in order to ensure that participating organisations meet the requirements of the GDPR, in accordance with Articles 5.1.f, 24, 25 and 32 of the GDPR;
 - d. taking technical and organisational measures to prevent consent from being ticked by default in the CMP interfaces as well as to prevent automatic authorisation of participating vendors relying on legitimate interest for their processing activities, in accordance with Articles 24 and 25 of the GDPR;
 - e. forcing CMPs to adopt a uniform and GDPR-compliant approach to the information they submit to users, in accordance with Articles 12 to 14 and 24 of the GDPR;
 - f. updating the current records of processing activities, by including the processing of personal data in the TCF by IAB Europe, in accordance with Article 30 of the GDPR;

- g. carrying out a data protection impact assessment (DPIA) with regard to the processing activities under the TCF and their impact on the processing activities carried out under the OpenRTB system, as well as adapting this DPIA to future versions or amendments to the current version of the TCF, in accordance with Article 35 of the GDPR;
- h. appointing a Data Protection Officer (DPO) in accordance with Articles 37 to 39 of the GDPR.

These compliance measures should be completed within a maximum period of six months following the validation of an action plan by the Belgian Data Protection Authority, which shall be submitted to the Litigation Chamber within two months after this decision. Pursuant to Article 100 § 1^{er}, 12° of the DPA Act, a penalty payment of 5.000 EUR per day will be due in case of failure to comply within the above-mentioned time limits.

- impose an administrative fine of 250.000 EUR on the defendant pursuant to Article 101 of the DPA Act.

This decision may be appealed before the Market Court, pursuant to Article 108(1) of the DPA Act, within a period of thirty days from its notification, with the Data Protection Authority as defendant.

(signed) Hielke HIJMANS
President of the Litigation Chamber

Summary Final Decision Art 60

Complaint

Administrative fine, Compliance order

EDPBI:BE:OSS:D:2022:325

Background information

Date of final decision:	02 February 2022
Date of broadcast:	02 February 2022
Controller:	Interactive Advertising Bureau Europe (IAB Europe)
Processor:	N/A
LSA:	BE
CSAs:	AT, CY, CZ, DEBY, DEBE, DEBB, DENI, DENI, DEMV, DENW, DERP, DESL, DK, EL, ES, FI, FR, HR, HU, IE, IT, LU, LV, NL, NO, PL, PT, SE, SI.
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), Article 7 (Conditions for consent) Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 13 (Information to be provided where personal data are collected from the data subject), Article 14 (Information to be provided where personal data have not been obtained from the data subject), Article 24 (Responsibility of the controller), Article 30 (Records of processing activities), Article 32 (Security of processing), Article 35 (Data protection impact assessment), Article 37 (Designation of the data protection officer)
Decision:	Administrative fine, Compliance order
Key words:	Advertising, E-Commerce, Profiling, Lawfulness of processing, Legitimate interest, Consent, Transparency, Data security, Data protection officer, Data protection impact assessment, Accountability, Data protection by design and by default, Record of processing activities.

Summary of the Decision

Origin of the case

The defendant is a federation representing the digital advertisement and marketing industry on the European level. This organisation has developed a Transparency and Consent Framework (TCF)

allowing to capture users' ads preferences in order to share them with organisations that take part in one of the most used "Real-Time Bidding" (RTB) protocols worldwide (publishers, consent management providers and other adtech vendors).

A RTB protocol is an automatic system allowing third-party companies to bid instantly for advertising space in order to display targeted ads specifically tailored to a user's profile. As a result, the user will be shown the ads of the company that offered the highest bid for the profile assigned to it.

Thanks to the TCF developed by the defendant, the organisations participating to this RTB protocol can be informed of what the user has consented or objected to, and thus know whether they have a legal basis for displaying their ads to this user.

Findings

As regards the nature of the data processed in the context of the TCF, the LSA noted that the TCF inevitably involves the collection of users' IP addresses which, when combined with other information held by the participants, makes it possible to identify the users who have expressed their preferences when visiting a website or an app. The LSA thus concluded that the data processed in the framework of the TCF qualifies as personal data.

Further, the LSA held that, although the defendant may not process nor access these personal data, it nevertheless exercises a decisive influence on the purposes of these processing. In addition, the LSA pointed out that the defendant is the one which defines the rules applicable to the processing and that those rules are imposed to the organisations participating in the TCF. As a result, the LSA found that the defendant, together with the other organisations participating to the TCF, is a joint controller for the processing related to the collection and dissemination of users' preferences, objections and consent, as well as for the subsequent processing of the users' personal data based on those preferences.

Moreover, the LSA found that the defendant did not provide a valid legal basis for the processing related to the registration of the consent signal, objections and users' preferences. As to the processing related to the collection and dissemination of user' personal data in the context of the RTB, it was established by the LSA that none of the legal grounds proposed and implemented by the TCF (i.e. consent or legitimate interest) could be lawfully invoked by the TCF participants. Thus, the defendant infringed Art. 6 GDPR.

Concerning the information provided to the users, the LSA observed that the information provided to data subjects was expressed in a too generic manner and did not enable them to understand the nature and scope of the processing carried out in the context of the TCF. The LSA therefore concluded that the defendant did not comply with the obligations under Articles 12, 13 and 14 GDPR.

Finally, the LSA found that the defendant failed to comply with several other of its obligations under the GDPR. These violations relate to the principle of accountability (Art. 24 GDPR), data protection by design and by default (Art. 25 GDPR), data security (Art. 5(1)(f) and 32 GDPR), the obligations to keep a register of processing operations (Art. 30 GDPR), to carry out DPIA (Art. 35 GDPR), as well as to appoint a DPO (Art. 37 GDPR).

Decision

The LSA imposed a €250.000 fine to the defendant. Additionally, it ordered the defendant to undertake a series of corrective measures in order to bring the processing carried out under the TCF into compliance with the GDPR. The LSA gave the controller two months to present an action plan to implement these corrective measures, and a maximum period of six months to complete the compliance measures indicated in the action plan, after validation thereof by the LSA.



COMMISSION FOR PERSONAL DATA PROTECTION

FINAL DECISION

Ref. № ПАИКД-13-28/2022

IMI A56 424363

The Commission for Personal Data Protection (CPDP, the Bulgarian SA) has initiated a procedure under Article 56 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR) in its capacity as supervisory authority competent to act as the lead supervisory authority for cross-border processing carried out by a controller established in the Republic of Bulgaria. The procedure was initiated by the CPDP on 2 September 2022 in the Internal Market Information System with number IMI A56 424363.

In connection with the above, at a plenary meeting held on 26 October 2022, the Commission, composed of: [REDACTED] (Chairperson) and [REDACTED] and [REDACTED] [REDACTED] (Members), considered a Statement of Findings, drafted by the Legal Analysis, Information and Control Directorate.

I. The Facts

The data controller LockTrip Ltd., with a National Identification Number: 204752244 (the company, the controller), submitted a personal data breach notification with the CPDP (№ ПАИКД-13-28/09.06.2022 г. pursuant Article 33 GDPR. The controller's single place of establishment is at 78 Alexander Malinov Blvd., Mladost 4 Residential Area, 1799, Sofia, Bulgaria. The controller is a company that provides services, related to software development and consultancy in the field of information technology. According to the information received, the personal computer of an employee of the controller (a call centre operator) was compromised by logging in to a public Wi-

Fi network. As a result of the breach, passwords for access to shared private spaces and platforms of partners of LockTrip Ltd. were leaked.

II. Actions taken by the CPDP after receiving the notification:

Pursuant to Article 62 of the Rules on the Activity of the Commission for Personal Data Protection and Its Administration (RACPDPA), the data breach notification was registered in the relevant internal register. Since the initial information in the notification form did not contain the minimum information required under Article 33 (3) GDPR, it was subsequently requested in the course of the administrative proceedings by letter (№. ПАИКД-13-28#1/16.06.2022 г.). The controller provided additional information by letters. №. ПАИКД-13-28#2/20.06.2022 г.#2 and №. ПАИКД-13-28#3/30.06.2022 г. Pursuant Article 63 of the RACPDPA, the notification was analysed on the basis of the Methodology for Risk Assessment upon a Personal Data Breach, adopted with a Decision of the Bulgarian SA of 24 June 2021. Further to the above, following a Decision of the CPDP from 6 July 2022 a document inspection was carried out in connection with the breach which had been brought to the attention of the supervisory authority.

The main task of the inspection was to ascertain the facts and circumstances related to the breach, the technical and organisational measures that had been taken before the incident, and to identify the possible omissions that had made possible for the breach to occur. Another task of the inspection was to ascertain the measures taken to mitigate the possible adverse effects and minimise the possibility of such an incident to occur again.

III. Analysis of the information provided in connection with the notification received and the actions taken:

1. Nature of the breach:

According to the information provided on 5 June 2022 the controller's monitoring systems, as well as its employees, detected suspicious and unauthorised activity. An on-duty employee was alerted by email from a partner platform of LockTrip Ltd. of a misapplied operating algorithm for hotel bookings. After the case was scrutinised, it was found that data security had in fact been breached. It was established that the personal computer of an employee of the controller (a call centre operator) was compromised by logging in to a public Wi-Fi network. As a result of the breach, passwords for access to shared private spaces and platforms of partners of LockTrip Ltd. including: Agoda, Booking, Dida Travel, DOTW, Escalabeds, Expedia, GetARoom, Go Global, GRNconnect, Hotelbeds, HotelDo, Hotelston, Hotusa, LotsOfflotels, Miki Travel, RateHawk, RTS, Stuba, SunHotels, TBOHolidavs, TotalStay, WelcomeBeds, were leaked.

There is no information showing and suggesting that the integrity of the data was compromised. The third party who committed the unauthorised access retrieved all data that they have accessed.

The number of personal data records affected by the breach is 2,199 unique records.

The number of data subjects (natural persons) affected by the breach is 2,025 data subjects.

If broken down by type of bookings: successful bookings, cancelled bookings, and attempted bookings.

Bookings where the arrival date is prior to the incident (5 June 2022): 2,046 unique emails from natural persons;

Bookings where the arrival date is after the incident (5 June 2022): 182 unique emails from natural persons.

The controller points out that 19 (nineteen) of the bookings affected indicated that there could be children aged under 14 will check in. Two of all the bookings affected specified the children's names and age.

The following categories of personal data were affected by the breach: names; address; email address; IP address from which the booking was made.

The persons affected by the breach include both EU citizens and third-country nationals.

Number of persons affected broken down by the value of the booking:

Bookings for an arrival date after the 5 June 2022 incident:

- from EUR 0 to EUR 100: 14 bookings;
- from EUR 100 to EUR 500: 70 bookings;
- from EUR 500 to EUR 1,000: 42 bookings;
- over EUR 1,000: 56 bookings.

Bookings for an arrival date before the 5 June 2022 incident (past bookings):

- from EUR 0 to EUR 100: 537 bookings;
- from EUR 100 to EUR 500: 893 bookings;
- from EUR 500 to EUR 1,000: 265 bookings;
- over EUR 1,000: 351 bookings.

In the data breach notification, the controller argues that the presence of personal data, such as names, address, email address and IP address from which the booking was made, could not be used for financial abuse or transactions.

The controller reports that users of the LockTrip Ltd. booking system, depending on the preferred payment method, are redirected to an external encrypted link of one of two payment processors: Stripe or CoinPayments. The employees of LockTrip Ltd. do not have access to sensitive information like bank card number or CVV/CVC code, while the respective booking is in progress.

The notification indicates that the breach has a significant potential impact on the data subjects whose names, addresses and forthcoming booking were leaked because they may be targeted by phishing attacks requiring additional payments for a booking or the submission of copies of an identity document or a payment instrument. It is possible that data subjects provide this information as it is normally associated with visits at hotels. The controller is of an opinion that the data subjects in question may be targeted by other attempts at criminal activity, considering that they are not present at their home. However, that would be hardly likely because it is quite possible that the potential third party is not present in a country where the data subject's permanent address is or in a country in which the data subject will reside during their booking.

LockTrip Ltd. notes that the breach has a limited potential impact on the data subjects whose names, addresses and past booking were leaked, however they could be targeted by phishing attacks requiring extra payments for a certain stay, but the effect of something like that could be less significant owing to the lower likelihood of the data subject being misled.

2. Designating the CPDP as the Lead Supervisory Authority

In addition, responding to the CPDP's query № ПАИКД-13-28#1/16.06.2022 г., by letter with № ПАИКД-13-28#6/20.07.2022 г. LockTrip Ltd. provided particular information regarding:

The number of persons who indicated their country of origin in their registration (applicable to bookings done before 5 June 2022):

AE (United Arab Emirates) 239; AM (Armenia) 1; AR (Argentina) 13; AT (Austria) 144; AU (Australia) 48; AZ (Azerbaijan) 1; BA (Bosnia and Herzegovina) 32; BD (Bangladesh) 1; BE (Belgium) 70; BG (Bulgaria) 396; BO (Bolivia) 3; BR (Brazil) 20; BS (Bahamas) 3; BY (Belarus) 9; CA (Canada) 96; CH (Switzerland) 57; CL (Chile) 24; CO (Colombia) 13; CR (Costa Rica) 14; CY (Cyprus) 27; CZ (The Czech Republic) 15; DE (Germany) 222; DK (Denmark) 22; DO (Dominical Republic) 10; EE (Estonia) 1; EG (Egypt) 16; ES (Spain) 141; FI (Finland) 29; FR (France) 108; GB (United Kingdom) 350; GE (Georgia) 3; GI (Gibraltar) 2; GM (Gambia) 3; GR (Greece) 16; T (Guatemala) 5; HK (Hong Kong) 8; HN (Honduras) 11; HR (Croatia) 422; HU (Hungary) 14; ID (Indonesia) 20; IE (Ireland) 69; IL (Israel) 10; IM (Isle of Man) 5; IN (India) 97; IR (Iran) 7; IS (Iceland) 3; IT (Italy) 90; JE (Jersey) 16; JM (Jamaica) 2; JO (Jordan) 8; JP (Japan) 22; KE (Kenya) 2; KH (Cambodia) 2; KR (South Korea) 4; LB (Lebanon) 1; LI (Liechtenstein) 1; LK (Sri Lanka) 4; LT (Lithuania) 3; LV (Latvia) 3; LY (Libya) 2; MA (Morocco) 6; MC (Monaco) 27; MD (Moldova) 1; ME (Montenegro) 10; MK (North Macedonia) 4; MN (Mongolia) 1; MO (Macao) 5; MT (Malta) 17; MX (Mexico) 30; MY (Malaysia) 17; NG (Nigeria) 5; NL (The Netherlands) 160; NO (Norway) 18; NP (Nepal) 4; NZ (New Zealand) 9; PA (Panama) 6; PE (Peru) 9; PH (Philippines) 3; PK (Pakistan) 3; PL (Poland) 21; PR (Puerto Rico) 4; PT (Portugal) 31; PY (Paraguay) 4; QA (Qatar) 24; RO (Romania) 14; RS (Serbia) 54; RU (Russia) 32; SA (Saudi Arabia)

2; SD (Sudan) 2; SE (Sweden) 82; SG (Singapore) 19; SI (Slovenia) 12; SK (Slovakia) 1; SV (El Salvador) 3; TH (Thailand) 44; TN (Tunisia) 10; TR (Turkey) 33; TW (Taiwan) 1; TZ (Tanzania) 1; UA (Ukraine) 14; US (The United States of America) 630; UY (Uruguay) 1; VE (Venezuela) 3; VN (Vietnam) 14; ZA (South Africa) 18.

and

the number of persons who indicated their country of origin in their registration (applicable to bookings after 5 June 2022):

AE (United Arab Emirates) 4; AT (Austria) 4; AU (Australia) 12; AZ (Azerbaijan) 1; BA (Bosnia and Herzegovina) 4; BE (Belgium) 7; BG (Bulgaria) 24; CH (Switzerland) 1; CO (Colombia) 1; CZ (The Czech Republic) 2; DE (Germany) 15; DK (Denmark) 4; EG (Egypt) 3; ES (Spain) 4; FR (France) 2; GB (United Kingdom) 40; HR (Croatia) 84; IE (Ireland) 4; IN (India) 1; IR JE (Jersey) 1; KR (South Korea) 1; MY (Malaysia) 1; NL (The Netherlands) 8; NO (Norway) 1; NZ (New Zealand) 3; PK (Pakistan) 1; PL (Poland) 1; PT (Portugal) 3; QA (Qatar) 2; RS (Serbia) 9; SE (Sweden) 2; SG (Singapore) 3; SI (Slovenia) 2; SK (Slovakia) 1; TN (Tunisia) 1; US (The United States of America) 11; ZA (South Africa) 18.

The EU citizens affected by the breach are 2,108, including 420 Bulgarian citizens.

The third-country nationals affected by the breach are 2,423.

The information as additionally received was presented at a plenary meeting of the Bulgarian SA on 27 July 2022 (Report № ПАИКД-13-28#7/25.07.2022 г.), pursuant to which the following decisions were adopted as recorded in Minutes of Proceedings before the CPDP № 31 of 27 July 2022:

1. The CPDP will assume the role of the lead supervisory authority as the main establishment or the single establishment of the controller is within the territory of the Republic of Bulgaria (Article 56 (1) GDPR).
2. The case would be registered in the Internal Market Information System (IMI), stating that the CPDP would assume the role of the lead supervisory authority, and brief information will be provided about the breach and the nationalities of the affected EU citizens.

The Commission for Personal Data Protection assumed the role of the lead supervisory authority under procedure IMI A56 424363. At the time of the drafting of the present decision, the supervisory authorities of Rhineland-Palatinate, the Netherlands, Lower Saxony, Italy, France, Brandenburg, Norway, Ireland, Austria, Belgium, Estonia, Romania, Sweden, Slovakia, Denmark, Finland and Spain have identified themselves as concerned supervisory authorities (CSAs).

On 2 December 2022, the Bulgarian SA launched an Article 60 procedure – draft decision IMI A60DD 464486. Within the established deadline only a comment by the Polish SA was received, stating that the authority was satisfied with the draft decision.

3. Actions taken by the data controller to restrict the breach:

- The data subjects were notified (by email) in order to be more vigilant about any messages sent to them in connection with their booking registrations. The affected persons were notified by email of the security breach. Information, regarding the type of data to which the third parties had gained access to, the way in which that data could be used against the data subjects (*phishing attacks, for example*), as well as how they could protect themselves. Also, on 8 June 2022 the Managing Director of LockTrip Ltd. published an official announcement in the LockTrip Telegram channel at the Telegram messenger platform, whose members are long-term investors, supporters and fans of the project;
- The compromised profile of the employee of the controller, as well as their personal computer were localised;
- The compromised profile of the employee of the controller was temporarily deactivated, and its access to all shared private spaces and partner platforms were blocked;
- The passwords for access to all shared private spaces and partner platforms were changed;
- An additional two-factor security verification for granting access to all shared private spaces and partner platforms was activated;
- Reinstalling and deleting all the information stored on the hard disk of the compromised personal computer; The employee of the controller whose personal computer had been compromised was provided with a new wireless internet router in order to enhance security.

4. Actions taken by the data controller to prevent a recurrence of the breach:

- Establishment of a new internal policy and procedure for security enhancement;
- Implementation of new methods for monitoring access to the shared private spaces and partner platforms;
- Delivery of internal technical training to all employees in order to raise their awareness of cyber security.

The initial analysis of the information provided with the notification was covered in a Report № ПАИКД-13-28#4/05.07.2022 г. The severity of the risk to the rights and freedoms of data subjects was determined according to the Methodology for Risk Assessment upon a Personal Data

Breach, adopted with a Decision of the Bulgarian SA from 24 June 2021. The rights and freedoms of the persons affected were found to be at “medium risk”.

IV. Analysis of the evidence presented in connection with the document inspection carried out:

In order to fully clarify all the circumstances relevant to the case, additional information was requested from LockTrip Ltd. by the CPDP with letters. № ПАИКД-13-28#8/26.07.2022 г. and № ПАИКД-13-28#15/02.09.2022 г.

In connection with the additional information requested, an exchange of correspondence took place between the Bulgarian SA and LockTrip Ltd. The controller requested an extension of the legally defined period of time for the provision of the abovementioned information: letters from LockTrip Ltd. № ПАИКД-13-28#9/27.07.2022 г.; № ПАИКД-13-28#10/02.08.2022 г.; № ПАИКД-13-28#16/12.09.2022 г. and letters, sent by the CPDP. № ПАИКД-13-28#12/03.08.2022 г.; № ПАИКД-13-28#18/26.09.2022 г.; № ПАИКД-13-28#19/27.09.2022 г.

The information as presented below was provided by the data controller with the following letters № ПАИКД-13-28#14/17.08.2022 г.; № ПАИКД-13-28#17/14.09.2022 г.; № ПАИКД-13-28#20/29.09.2022 г.; № ПАИКД-13-28#21/03.10.2022 г.:

- In its response with letter № ПАИКД-13-28#14/17.08.2022 г., the controller indicated that the cause of the incident had been identified as a result of an internal inspection that has been carried out. An employee of LockTrip Ltd., who was subsequently identified, had logged in to a public Wi-Fi network, and the LockTrip's systems were therefore made available externally. The inspection has furthermore identified the individual whose personal computer had been compromised after the malicious attack, where shared private spaces were subjected to unauthorised access, and where partner portals of LockTrip Ltd. had been subjected to unauthorised access. Written evidence ascertaining the conduct of the internal inspection (reports, conclusions, etc.) was not presented together with the official statement of the controller.

- With regard to whether the controller delivers training in personal data protection to its employees and, hence, to present evidence, the controller stated that before taking the respective position, the persons who are responsible for safeguarding and processing personal data have the obligation not to disclose the personal data to which they have access to and not to share critical information with each other and with third parties. Follow-up training sessions of the staff are held periodically so as to ensure familiarity with the regulatory framework, the potential risks to data security, as well as the measures for their reduction. Evidence was not presented.

- The controller notes that by the date of the breach they did not consider that requirements under Regulation (EU) 2016/679 were available for analysing the risk to the rights and

freedoms of natural persons with regard to the processing of their data. Therefore, no such analysis was carried out before the data breach. A Data Protection Impact Assessment for the Personal Data Processed by the Controller LockTrip Ltd. was presented with letter № ПАИКД-13-28#14/17.08.2022 г.

- With regard to the conduct of a prior audit of the information systems, the controller states that a DEV team checks the information systems on a weekly basis, monitoring a series of records, indicators and values. They are intended to establish whether the overall system functions as intended, whether any of its components exhibits a deviation or technical failure and, last but not least, whether there is a breach of security, the operating algorithm and the authorised access. The controller did not specify whether the checks involve an analysis and audit of the technical and organisational measures taken for the protection of personal data when using remote access, because the present case concerns a security breach that occurred precisely for this reason.

- Regarding the matter of enclosing the evidence collected and analysed of each fact established, namely paper and/or electronic documents (including rules, procedures, instructions, official statements, print screens, etc.), LockTrip Ltd. pointed out in their official statement: “As the CPDP has not thus far requested the so-called “server logs”, nor a request for their retention has been sent, their 40-day retention period had expired by 26 July 2022. Accordingly, no collected and analysed evidence whatsoever can possibly be provided as of today’s date. All data, concerning the breach were perused and analysed in real time on our server. The reason why nothing is retained is that the ‘server logs’ in question contain sensitive information which is archived over a definite time interval in order to safeguard its security.”

Considering the fact that the additional information sent to the Bulgarian SA (letter № ПАИКД-13-28#14/17.08.2022 г.) does not make it possible to clarify all facts and circumstances relevant to the present case, the controller was requested again to present written statements (letter with № ПАИКД-13-28#15/02.09.2022 г.), enclosing the relevant documents and evidence ascertaining the actions taken with regard to:

- LockTrip Ltd.’s Rules on employees’ access to the company’s platforms;
- What alert systems have been implemented by the company for attempts of unauthorised access at infrastructure level and at employee level;
- Training materials on personal data protection, compiled and intended for the company’s employees, both with regard to their initial training and to the follow-up periodical trainings;
- Written evidence of training in personal data protection delivered to the employee whose personal computer was subjected to a malicious attack (for example, a certificate, an attendance form, a test form, etc.), as well as a declaration by the said employee to the effect that

they have been trained and made familiar with the company's rules concerning personal data protection;

- Considering the information that the personal data are processed in electronic form on computers located at the employees' homes, a specification of the location where the personal data of the data subjects affected by the breach are stored and processed should be provided;

- In connection with the information submitted by LockTrip Ltd. that the 'server logs' had not been requested by the CPDP thus far nor a request had been made for their retention and that they had been destroyed due to the expiration of the period of 40 days , the controller's attention was drawn to the fact that, pursuant to Article 5(1)(f) in conjunction with Article 5(2) of Regulation (EU) 2016/679, the controller is responsible for and is expected to be able to demonstrate (principle of "accountability") that they process the data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (principle of "integrity and confidentiality"). Considering the above, the Bulgarian SA explained that LockTrip Ltd. had to demonstrate compliance with the principles of 'accountability, integrity and confidentiality' with regard to the particular incident that had occurred. Since the CPDP did not have specific information on the internal documents by which the controller was able to demonstrate compliance with the principles at its disposal, it could only point out that LockTrip Ltd. was supposed to present the evidence they had collected and analysed (after the conduct of the appropriate internal inspection) of each fact established in connection with the incident: paper and/or electronic documents (including rules, procedures, instructions, official statements, print screens, etc.. The controller was reminded that the abovementioned, as described had already been requested by letter № ПАИКД-13-28#15/26.07.2022 г. and by that point the controller is invited again to present the appropriate relevant evidence.

- Furthermore, the controller's attention was drawn to the fact that, according to Article 24 (1) and (2) of Regulation (EU) 2016/679, it is expected to take into account the nature, scope, context and purposes of the specific personal data that they process. In this regard, the controller must consider the risks of varying likelihood and severity for the rights and freedoms of natural persons, responding to such risks by implementing appropriate technical and organisational measures, and has also be able to demonstrate their implementation. Considering the above, the Bulgarian SA needs to be informed of the technical and organisational measures for data protection (referred to in the relevant internal documents) that had been taken before the incident occurred.

In response to the CPDP's letter, the controller provided additional information and documents (by letter № ПАИКД-13-28#17/14.09.2022 г.):

- The controller presented *Rules on LockTrip Ltd. Employees' Access to Internal Information Systems and Partner Portals of the Organisation*, endorsed by the Managing Director

of the Company (Ref. No. 20210108 of 1 August 2021). No evidence has been provided as to how employees were made aware of the Rules in question.

- A document entitled *Monitoring of and Access to Internal Information Systems and Shared Partner Platforms* was presented, as endorsed by the Managing Director of the company (Ref. No. 20210108-3 of 1 August 2021). The document, which every employee, including the members of the operational department of LockTrip (*call centre operator and contact centre manager team*) are obliged to observe and comply with, lays down the methods for monitoring, and the access at architecture and agent level to the internal information systems and shared partner platforms. No evidence has been provided as to how employees were made aware of the document in question.

- With regard to the training materials requested by the CPDP that had been used to familiarise employees with the rules on personal data processing, the controller presented a document entitled *European Policies and Personal Data Protection Regulation*, which describes the general provisions introduced with Regulation (EU) 2016/679. The document ends with open-ended questions for self-study:

- ✓ When does the *GDPR* enter into force?
- ✓ What does the Personal Data Protection Act regulate in the Republic of Bulgaria?
- ✓ Define *personal data*.
- ✓ Which are the areas of data processing specified in the *GDPR*?
- ✓ What is the other name of the right to erasure?
- ✓ Which is the most important principle of the *GDPR*?

A further examination and analysis of the content of the document establishes that it does not contain rules, which employees are supposed to follow when processing personal data in connection with the specific activity of LockTrip Ltd. No evidence was presented in order to ascertain that the employees had been made familiar with the document or that they had provided an answer to the open-ended questions for self-study.

- The controller presented *Internal Work Rules of LockTrip Ltd.*, intended to regulate matters related to work discipline, an appropriate organisation of work, and the full and effective utilisation of working hours. In terms of content, the provisions of the document presented as evidence are irrelevant to the present case concerning the matters of personal data processing. As the document itself states, the Rules were drawn up pursuant of Article 181 of the Labour Code.

- The controller presented Order No. 0000005 of 6 December 2021, issued pursuant to Ordinance No. 15 of 31 May 1999 on the Terms, Procedure and Requirements for the Development and Introduction of Physiological Patterns of Work and Rest during Work and Article 151 of the Labour Code. This order, is irrelevant as evidence, as well.

- The controller presented a *Declaration on Compliance with the Requirements for*

Health and Safety at Work. It was pointed out that the declaration was signed on 14 January 2022 by the employee, whose personal computer was compromised as a result of logging in to a public Wi-Fi network.

The declaration reads that the employee: *Has been familiarised with the company's health and safety rules, as well as with established physiological work and rest regime for the activity they perform. They The employee will comply with all the requirements, procedures, technical rules, obligations of confidentiality and health and safety rules related to the performance of work and approved by the company, as well as the health and safety rules prescribed to them in connection with remote working; They will organise their workplace so as to satisfy the minimum health and safety requirements laid down in the Health and Safety at Work Act and in the legal instruments for its application , as well as according to the company's rules on work with displays , will comply with the requirements for working hours and the physiological patterns for work and rest for the type of activity which the employee carries out.*

The declaration presented is irrelevant as evidence to the present case.

- The controller presented WORK CERTIFICATE No. 004 of 4 January 2022, showing that the employee received an initial training on 4 January 2022, however it does not specify its type. The reference is presumably to the *Declaration on Compliance with Requirements for Health and Safety at Work* as described above.

Additionally, LockTrip Ltd. sent the following by letters with № ПАИКД-13-28#20/29.09.2022 г. and № ПАИКД-13-28#21/03.010.2022 г.:

- Partner agreements with Agoda Company PTE LTD and Booking.com BV;
- An internal procedure concerning the cancellation and refund process;
- An internal procedure concerning issues related to the payment process on the customer side;
- An internal procedure concerning the process of hotel booking confirmation;
- An internal procedure concerning issues related to hotel mapping;
- An internal procedure concerning issues related to hotel room mapping;
- Internal procedure concerning manual reservation “rescue”;
- An internal procedure concerning a booking flow and email notifications;
- Established rules on the access of the employees of LockTrip Ltd. to the internal information systems and partner portals of the organisation.

The controller presented an annex to the partner agreement with Agoda Company PTE LTD regulating the relationships between the partners with regard to the personal data processing for the purposes of the agreement. Point 11 of the agreement with Booking “CONFIDENTIALITY AND SECURITY” includes clauses regulating the lawful processing of personal data for the purposes of

the agreement between the partners.

Regarding the additionally presented Internal Procedures as described above, they cannot be considered evidence relevant to the present case.

V. Conclusions of the CPDP after conducting the document inspection:

1. Based on the findings of the document inspection, it was established that LockTrip Ltd., in its capacity as “personal data controller” within the meaning of Article 4(7) of Regulation (EU) 2016/679, allowed a security breach while carrying out its activity, namely: On 5 June 2022 the controller’s monitoring systems and its employees detected suspicious and unauthorised activity. An on-duty employee was alerted by email from a partner platform of LockTrip Ltd. of a misapplied operating algorithm for hotel bookings. After the case was scrutinised, the controller found that data security had been breached. Even though the controller stated in the information provided, regarding the case file (without presenting evidence, such as audit reports, findings of the auditing team, etc.) that before the security breach the information systems had been audited on a weekly basis by a DEV team in order to monitor whether the overall system functioned as intended, and whether any of its components exhibited a deviation or technical failure and, last but not least, whether there was a breach of security, the operating algorithm and the authorised access, the security breach as described in personal data breach notification № ПАИКД-13-28/09.06.2022 г. demonstrates that the technical and organisational measures taken by the controller were inappropriate. When determining which measures are appropriate, the controller should take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. After making such an assessment and analysis, the controller should apply appropriate technical and organisational measures to ensure a level of security appropriate to the particular risks. In practice, the controller failed to ensure the security of the personal data being processed. The data controller found out about the breach after an email notification was received from a partner platform of LockTrip Ltd., which alerted them of a misapplied algorithm for hotel bookings, resulting in an unauthorised access and unauthorised disclosure of personal data: (names; address; email address; IP address from which the booking was made) of 2,108 EU citizens, including 420 Bulgarian citizens, and 2,423 third-country nationals.

Initially, the controller reported that by the time of the breach they did not consider that conditions under Regulation (EU) 2016/679 were available for analysing the risk to the rights and freedoms of natural persons with regard to the processing of their data. Therefore, no such analysis was carried out before the security breach. A Data Protection Impact Assessment for the Personal Data Processed by the Controller LockTrip Ltd. was presented additionally by letter № ПАИКД-

13-28#14/17.08.2022 r. The document as presented, points out that, in the opinion of the company, the processing of personal data on their part does not pose a high risk to the rights and freedoms of data subjects but, considering a security breach detected in June 2022, a decision was made to prepare an Impact Assessment concerning clients' personal data that have been processed by the company. By way of addressing the risks, the company took the following measures:

1.1 Two-factor authentication (2FA) as a key protection and security measure. It requires from an employee to provide two different pieces of information in order to prove who they are before access is granted. This is a security protocol which essentially provides an extra layer of security in addition to the user's password, in cases where the password is compromised. When a user tries to access an account, they will be asked to enter their user name and password plus 2FA codes. Then the user will receive a text message with a six-digit passcode that they must enter in order to complete the entry process. The user sends the code from their phone, and so the person who has accessed the account never possesses the code.

1.2 Any outside access to the system on the part of employees has been restricted. In extreme necessity, such access is granted after the submission of a notifying request which indicates:

- specific reasons for the need to grant an outside access to the system;
- IP address from which the system will be accessed;
- period of time (*days, weeks, etc.*) for which the need to grant outside access to the system applies.

After considering the abovementioned, the Managing Director of LockTrip Ltd. makes a reasoned decision to allow or reject the submitted request.

1.3 A LastPass Premium service has been implemented, which makes it possible:

- to create a LockTrip master account controlling the access to all passwords (*including shared private spaces and partner portals*);
- to add or to cancel agent access to shared private spaces and partner portals at any time;
- to "destroy" all web sessions of an agent at any time: by this step the agent will be automatically logged out from all active sessions, regardless of the number and types of devices using LastPass;

1.4 Email notification of an unauthorised access attempt, and push notification to the mobile device linked to the relevant user profile.

2. It is important to note that, according to Article 33(5) of Regulation (EU) 2016/679, the controller should document all facts relating to the personal data breach, its effects and the remedial action taken. That documentation enables the supervisory authority to verify the compliance of the controller with the cited provision of the Regulation. In this particular case, the controller failed to provide documents and evidence that are important for the proceedings, even though the CPDP

repeatedly requested these documents and evidence in the correspondence exchanged in connection with the examination of the personal data breach notification.

- In the personal data breach notification, the controller states that, for the purpose of preventing the breach to occur again, by 10 June 2022 they will adopt a new internal policy and procedure for security enhancement; will implement new methods for monitoring access to shared private spaces and partner platforms; will deliver internal technical training to all employees in order to raise their awareness of cyber security. While an examination of the breach was in progress and in the correspondence exchanged in this regard, no evidence of honouring the commitment assumed by the controller was presented to the CPDP. The internal rules relevant to personal data protection that were presented date from 2021;
- No factual evidence whatsoever was presented to ascertain that the controller's employees have been familiarised with the internal documents introducing rules on the lawful processing of personal data or that they have gone through initial training, as well as periodical training sessions concerning personal data protection (e.g. attendance forms, examination tests, declarations by the persons to the effect that they are familiar with the rules of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, etc.);
- No factual evidence whatsoever was presented to ascertain that the employee, holding the position of call centre operator, whose personal computer had been compromised as a result of logging in to a public Wi-Fi network, has received training, related to personal data protection. This resulted in the leak of passwords for access to shared private spaces and platforms of partners of LockTrip Ltd., including: Agoda, Booking, Dida Travel, DOTW, Escalabeds, Expedia, GetARoom, Go Global, GRNconnect, Hotelbeds, HotelDo, Hotelston, Hotusa, LotsOfflotels, Miki Travel, RateHawk, RTS, Stuba, SunHotels, TBOHolidavs, TotalStay, WelcomeBeds.

In relation with what is pointed in Section 2, it can be concluded that the controller failed to demonstrate compliance with Article 5 (1) of Regulation (EU) 2016/679, thus violating the “principle of accountability” under Article 5(2) in conjunction with Article 33(5) of Regulation (EU) 2016/679.

3. As mitigating circumstances, account should be taken of the fact that the controller notified the Bulgarian SA without undue delay, within 72 hours after having become aware of the breach; The data subjects, were notified via email sent to their email addresses, as well; This is a first personal data breach notification by that controller, regarding the personal data processed; The controller took action to limit the damage by temporarily deactivating the compromised profile of the employee and blocking their access to all shared private spaces and partner platforms; The passwords for access to all shared private spaces and partner platforms were changed; An additional

two-factor security verification was activated for access to all shared private spaces and partner platforms; The entire information stored on the hard disk of the compromised personal computer was reinstalled and deleted; The employee whose personal computer had been compromised was provided with a new wireless internet router in order to enhance security.

VI. Legal analysis

Regulation (EU) 2016/679, which was applicable since 25 May 2018, is the legal instrument laying down the rules related to the protection of natural persons with regard to the processing of personal data. The GDPR builds on the previous data protection legal framework introduced with Directive 95/46/EC, which was transposed into the Bulgarian Personal Data Protection Act of 2002 while, at the same time, takes account of the vigorous development of new technologies and of personal data processing activities.

According to the legal definition pursuant to Article 4(12) of the GDPR, “*personal data breach*” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. In this particular case, unauthorised access was gained through the personal computer of an employee of the controller which had been compromised because of logging in to a public Wi-Fi network. As a result, passwords for access to shared private spaces and platforms of partners of LockTrip Ltd. were leaked.

The controller is obliged to take the appropriate technical and organisational measures for protection of the data, as well as to establish mechanisms for control of their implementation, and thus demonstrate compliance with the provisions of the GDPR.

The CPDP has a broad discretion and, in accordance with the functions conferred thereon, assesses which of the corrective powers under Article 58(2) of Regulation (EU) 2016/679 to exercise. The assessment is based on considerations of appropriateness and effectiveness, taking account of the specificities of each particular case and the extent to which the interests of the data subjects concerned are affected, as well as the public interest. The powers under Article 58(2), excluding those pursuant to letter (i) GDPR, are of the nature of coercive administrative measures intended to prevent or to cease the conduct of an infringement, thereby achieving due diligence in the field of personal data protection.

In applying the appropriate corrective measure under Article 58(2) of the GDPR, account is taken of the nature, gravity and consequences of the breach, as well as all mitigating and aggravating factors. The assessment of what measures are effective, proportionate and dissuasive in each individual case also reflects the objective pursued by the corrective measure selected: a prevention

or termination of the breach, sanctioning the unlawful conduct or both, which is a possibility provided for in letter (i) of Article 58 (2) of Regulation (EU) 2016/679.

Considering the present case, the CPDP takes account of the facts and, more specifically, the insufficient technical and organisational measures that allowed vulnerability, namely a breach of security through the personal computer of an employee of the controller due to its connection to a public Wi-Fi network, as well as the results of the document inspection conducted, which certified that additional action had been taken for the prevention of such incidents, taking account of the nature, gravity and possible consequences of the personal data breach.

Considering the above, after a review and analysis of all the evidence collected in the administrative case file, for the purpose of preventing such breaches in the future, the Commission for Personal Data Protection has adopted the following

FINAL DECISION

- 1.) Pursuant to letter (b) of Article 58(2) of Regulation (EU) 2016/679, for an infringement of letter (f) of Article 5(1) in conjunction with letter (b) and letter (d) of Article 32(1), the Commission hereby *issues a reprimand to LockTrip Ltd.* for allowing infringements of the provisions of the Regulation under Personal Data Breach Notification. № ПАИКД-13-28/09.06.2022 г;**
- 2.) Pursuant to letter (d) of Article 58(2) of Regulation (EU) 2016/679, for a breach of the “principle of accountability” pursuant Article 5(2) in conjunction with Article 33(5) of Regulation (EU) 2016/679, the Commission hereby *orders LockTrip Ltd.* to bring its processing operations in compliance with the provisions of the Regulation by means of applying appropriate technical and organisational measures of data protection against unauthorised access such as:**
 - To analyse and audit the technical and organisational measures taken for the protection of personal data when using remote access;
 - To draft rules/a policy regulating the use of remote log-in to the company’s information systems, envisaging an automatic denial of access when logging in to a public Wi-Fi network;
 - To draft internal rules/procedures/instructions regulating the delivery of training in data protection (initial and periodic) and envisaging mechanisms for control of compliance. As part of the rules, a requirement should be included that when training to employees is delivered, the “principle of accountability” is to be respected and the controller must have evidence at their disposal (when inspected

by the CPDP) of the training sessions held, the employees who attended and the training materials;

- In connection with the infringement concerned, to deliver training in personal data protection to all employees and to present evidence of the said delivery, including signed attendance forms and training materials used in the training as delivered.
- 3.) This order is to be executed within 3 (three) months after the entry into effect of the Decision, and the controller will notify the Commission for Personal Data Protection of the execution within 14 (fourteen) days thereafter, presenting the relevant evidence.

The Decision of the Commission for Personal Data Protection could be appealed before the Sofia City Administrative Court within 14 (fourteen) days after receipt.

CHAIRPERSON:

[REDACTED]
(Signature)

MEMBERS:

[REDACTED]
(Signature)

[REDACTED]
(Signature)



REPUBLIC OF SLOVENIA

INFORMATION COMMISSIONER

Dunajska cesta 22, 1000 Ljubljana

T: 01 230 9730

www.ip-rs.si

gp.ip@ip-rs.si

National number: 06110-413/2022

IMI Case Register entry: 469543

Date: 8. 3. 2023

The Information Commissioner (hereinafter: IP) issues under the State Supervisor for Personal Data Protection [REDACTED] on the basis of Articles 2 and 8 of the Information Commissioner Act (Official Journal of the Republic of Slovenia, No. 113/2005, with amendments and additions; hereinafter: ZInfP), Articles 36 and 37 of the Personal Data Protection Act (Official Journal of the Republic of Slovenia, No. 163/22; hereinafter: ZVOP-2), Articles 57 and 58 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: GDPR), Article 135(4) of the General Administrative Procedure Act (Official Journal of the Republic of Slovenia, No. 24/06 — UPB2, 126/07, 65/08, 8/10, 82/13, 175/20 — ZIUOPDVE and 3/22 — ZDeb; hereinafter: ZUP) in conjunction with Article 3(2) of the Inspection Act (Official Journal of the Republic of Slovenia, No. 43/07 — UPB1 and 40/14; hereinafter: ZIN), in the matter of carrying out inspections of the implementation of the provisions of the GDPR and the ZVOP-2 at [REDACTED] (hereinafter: the controller), ex officio the following

DECISION

1. The inspection procedure conducted by the IP against the controller under No. 06110-413/2022 is terminated.
2. No specific costs were incurred in this procedure.

Findings and reasoning

The IP initiated the inspection procedure against the controller ex officio on the basis of a notification of a personal data breach (hereinafter: DBN), which has been sent to IP by the controller on 11 September 2022 in accordance with the provisions of Article 33 of the GDPR. The suspicion of inadequate insurance arose from the statements of the operator in DBN. The controller states that on 9 September 2022 he found that there had been a hacking (including [REDACTED] ransomware) attack on the controller's information system, that the extent and consequences of the attack were still being determined, as the analysis of the security incident had not yet been completed.

The inspection procedure was initiated on the basis of the Personal Data Protection Act (Official Gazette of the RS, no. 94/07-UPB1 and 177/20, hereinafter ZVOP-1), and in the meantime ZVOP-2 was adopted, which in the Article 119(1) stipulates that inspection procedures initiated on the basis of ZVOP-1 shall continue in accordance with ZVOP-2.

The controller provided very little information in the DBN. The State Supervisor for Personal Data Protection conducting the inspection procedure in question (hereinafter: the Supervisor), aiming to obtain more information about the controller, his services, the scope of business, the processing of personal data, and in order to be able to assess what obligations the IP as a Supervisory Authority has as a result of the DBN received in cross-border cooperation procedures under the GDPR, had carried out a review of the controller's website [REDACTED] on 13 September 2022.

Due to the need to clarify the case and establish the facts, on 15 September 2022 the IP requested the controller (hereinafter: request of the IP) to provide a written explanation, documentation and statement regarding the provision of information security in general and the security of personal data at the controller and regarding the handling of the security incident in question.

On 23 September 2022 the IP received a request from the controller for an extension of the deadline for reply, in which he explained that he was still intensively remedying the consequences of the hacking attack which partially paralyzed the controller's business and that his primary focus in this situation was to provide basic services to subscribers. The Supervisor complied with the controller's request and extended the deadline for replying to 17 October 2022.

IP received the response of the controller on the 17 October 2022. The controller replied to all the questions and attached the documents to which he referred in his answers. After examining the replies of the controller and the accompanying documentation, the Supervisor concluded that the controller had still not provided sufficient information and evidence to assess the appropriateness of the measures for the protection of personal data and the obligations of the IP as the lead supervisory authority in the cooperation procedure under the GDPR. In order to obtain all the necessary information and explanations, the Supervisor decided to hold a meeting with the controller, which was held on 8 November 2022.

Affiliated companies in the [REDACTED] are listed in Article 1 of the Personal Data Protection Regulations, which the controller provided in response to the IP request. In addition to the controller, the [REDACTED] also consists of:

- [REDACTED] Croatia,
- [REDACTED] Germany,
- [REDACTED], Italy,
- [REDACTED], Serbia,
- [REDACTED], Bosnia and Herzegovina,
- [REDACTED] Macedonia.

Currently, about [REDACTED] individuals are employed in all affiliated companies, of which [REDACTED] are employed at the controller. In companies outside Slovenia only affiliations in Croatia and Serbia have employees, the remaining companies are without employees. The affiliated companies have a common human resources management system (hereinafter: the HR system). The controller and the affiliated company in Croatia also use a common system for recording working hours [REDACTED]. In the HR system, in addition to the data of the employees of the controller, only the personal data of individuals employed in affiliated companies are recorded. To manage employee data in accordance with the requirements of labour law, each related company uses its own solutions adapted to the requirements of national law. Affiliated companies, which have employees, also independently take care of the purchase and maintenance of the computer equipment used by the employees. All other processing of personal data, where the controller acts as a controller or processor of personal data of his customers, is centralised.

All affiliated companies use a common process management system (hereinafter: [REDACTED]), that is, accounting and invoicing for the services of the controller is centralised. This system was attacked. The clients of the controller are only legal persons, but in the [REDACTED] system there are also contact details of employees (individuals) for the purpose of communicating with customers. All affiliated companies also use a common customer relationship management system (hereinafter: CRM system). The CRM system is a web solution that has not been attacked.

The services of the controller are also centralised. Servers, which are also accessed by clients and processors, are hosted by [REDACTED] (only the rental of secure premises). The customer's services are based on vehicle location data, other vehicle data (temperature, fuel level, door, etc.) and on tachograph data from drivers (traffic routes, vehicle,.ddd files). Customers do not see the driver's data until they have entered a request for an inspection (the driver's name and surname). The data is stored on the driver card (.ddd files) and is readable by special programs.

Users log in to the controller's network with a username and password. The controller uses the [REDACTED] login to the system. There are [REDACTED] with administrative rights, and these [REDACTED] have shared rights and do not use [REDACTED] computers. Around [REDACTED] users access the system remotely, using only computers owned and maintained by the controller.

The controller has conducted an internal investigation of the security incident and informed the parties that employ (or are in a contractual relationship with) the individuals whose personal data was compromised during the attack about the findings and the measures taken. The contact information of these individuals is available

only to the customers of the controller. Employees of the controller and affiliated companies were informed by the controller himself. Information on the security incident for affiliated companies, which was also submitted to the IP, was prepared by the controller in English.

The results of the internal investigation confirmed that the following servers of the controller's IT system (Office segment) were affected by the attack:



Two servers were affected in the service part (Production segment), namely:

- [REDACTED], e.g., from driver to dispatcher or from dispatcher to dispatcher). No data on recipients and senders were stored on this server or pseudonymised. The data that would allow de-pseudonymisation was located on a server that was switched off on time and the attackers had no access to it.
- [REDACTED] (contains temporary storage of application files, e.g., scanned accounts, CRM, photographs sent by drivers to dispatchers).

The controller did not agree to the demands of the attackers, but immediately after the attack was detected, he took a series of measures to protect the attacked system. The entire infrastructure and servers (whether attacked — encrypted or not) were turned off, formatted and reinstalled.

No data in the service part of the IT system was lost, so the controller was able to provide services to its customers within a few hours, while the other parts of the IT system were gradually restored.

As explained by the controller in response to the IP request, in order to prevent the possibility of re-intrusion to the same attackers, he also re-established the entire network, so that the attackers no longer have any advantage they would otherwise derive from their knowledge of the controller's IT architecture. He also carried out a series of additional measures to improve information security, about which, together with other information about the attack, he informed his partners.

Increased information security was also an explicit requirement prior to the transfer of ownership of the company. New owners [REDACTED] are also planning an external IT audit of the company's work and regular (including unannounced) penetration tests.

In the inspection process, it was not established which vulnerability the attacker has used to infiltrate the system. As the controller explained in his response to the IP request, the it considers that the intrusion started with the entry into the [REDACTED] server, as it found the first [REDACTED] installed on that server (according to the date of creation). Whether the attacker has taken advantage of any of the "zero-day" vulnerabilities of the [REDACTED] or has provided access to the system via a phishing message, is unlikely to be established as the attacker has deleted all traces.

The controller informed the IP, the Slovenian Computer Emergency Response Team (SI-CERT) and the Police about the attack. SI-CERT provided information which merely confirmed the conclusions reached by the controller himself and acted accordingly. On the 21 September 2022, the controller received a reply from the Police that a criminal investigation is being conducted

In the context of the analysis of the security incident, the controller did not detect increased traffic on the network or on the main switch of the network. Although at this moment, there are no indications that personal data has been disclosed or otherwise provided to third parties, the controller checks on a daily basis whether the personal data to which the attacker had access is published on the internet (including on the dark web) and has not detected the posts until now.

After examining the explanations provided by the controller and the documentation submitted, the IP found that, despite the fact that the breach in question did not pose a significant risk to the rights and freedoms of individuals whose personal data were compromised at the time of the attack, the controller had informed all affected individuals or partners who have contact details of those individuals of the consequences of the cyberattack, in accordance with the provisions of Article 34 of the GDPR, that the controller took appropriate measures to prevent such breaches in the future and to ensure the security of processing of personal data is in accordance with the provisions of Article 32 of the GDPR.

Since, in accordance with Article 4(23) of the GDPR, cross-border processing of personal data took place in the EU in the context of the activities of the sole establishment of the controller where the processing significantly affects or is likely to significantly affect data subjects in more than one Member State, the IP conducted the procedure in accordance with the rules on cross-border cooperation and compliance, as regulated by Sections 1 and 2 of Chapter VII of the General Regulation (in particular Articles 56 and 60 of the GDPR). On 27 December 2022, within the framework of the mutual assistance procedure (61VMN 469549), the IP informed the Supervisory Authority of Croatia as the concerned supervisory authority with the findings of the inspection procedure and the draft decision. Article 60 Draft Decision procedure (A60DD 484323) was launched on 7 February 2023. However, no relevant and reasoned objections were raised.

Since the suspicion of inadequate protection of personal data was not confirmed in the framework of the inspection procedure, the IP terminated the present procedure on the basis of Article 135(4) of the ZUP in conjunction with Articles 36 and 37 of the ZVOP-2 and Article 3(2) of the ZIN, as stated in point 1 of the operative part of this Decision.

Under the third paragraph of Article 118 of the ZUP, the costs of the proceedings are to be decided in the decision terminating the proceedings. In the present proceedings, no special costs have been incurred, as is apparent from point 2 of the operative part of this Decision.

This Decision is issued ex officio and on the basis of Article 22 of the Administrative Fees Act (Official Journal of the Republic of Slovenia No. 106/10 — official consolidated text, 14/15 — ZUUJFO, 84/15 — ZZelP-J and 32/16) the fees are free.

Instruction on Remedies: There is no appeal against this decision, but an administrative dispute is allowed. The administrative dispute is initiated by an action, which is filed within 30 days of service of the decision at the Administrative Court of the Republic of Slovenia, Fajfarjeva 33, 1000 Ljubljana. The application is sent by registered mail to that court. The action, accompanied by any annexes, shall be filed at least in triplicate. The application must also be accompanied by this order in original or transcript.

[REDACTED]
State Supervisor for Personal Data Protection

Recipient:
[REDACTED]

REPUBLIC



OF CYPRUS

*OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA PROTECTION*



Ref: 11.17.001.007.032 (1)

October 21, 2022

Varvelia Technologies Ltd
hello@netorsltd.com

Decision

Complaint against the website pickaflick.co by Varvelia Technologies Ltd (previously Netors Investments Ltd)

The complainant has lodged a complaint with the Spanish Data Protection Agency (Spain SA) on 21/12/2018 against Netors Investments Ltd, which administers the website <https://pickaflick.co/> (the “Controller”) and was received by the Office of the Commissioner for Personal Data Protection (“Cyprus SA” or “Commissioner”) according to the provisions of the cooperation and consistency procedures of the General Data Protection Regulation (EU) 2016/679 (the “Regulation”).

2. In line with Article 56 or the Regulation, the Commissioner is acting as the lead supervisory authority, as the Controller has its establishment in Cyprus.

Summary of the complaint:

3. The complainant stated, among others, that the Privacy Policy of the website <https://pickaflick.co/> states that the user has to consult periodically the website in order to learn about any changes and updates regarding the user’s data processing. The policy specifically stated the following:

“We may periodically make changes to this Privacy Policy and will notify you of these changes by posting the modified terms on the Website. We recommend that you revisit this

Privacy Policy regularly. If we are going to use Personal Information in a manner materially different from that stated at the time of collection, we will notify you by posting a notice on our Services. You may determine when this Privacy Policy was last updated by referring to the date found at the top of the first page of this Privacy Policy "This Privacy Policy was last modified and is effective as of".

4. The other parts of the complaint that concerns the use of cookies by the website, were handled outside the One Stop Shop mechanism, based on the national law that transposes the e-Privacy Directive and a separate Decision is issued.

Legal Framework

5.1. Based on Article 12 of the Regulation, the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

5.2. According to Article 13, where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject the information specified in Article 13.

5.3. Based on Article 13(3), when the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

Examination of the complaint

6. The Commissioner has informed the Controller regarding the alleged infringement of the provisions of the legislation and asked for his views/positions on the subject.

7. The Controller has made changes to the Privacy Policy, which now states that in case of changes to the policy, the users will be informed by email. Specifically the policy now states the following:

"For important reasons, we may periodically be required to make changes to our Privacy Policy (for example if we substantially change the way our services or the Website functions, or following legislative changes). We will notify you of these changes by e-mail and by posting the modified Privacy Policy on the Website".

8. It is noted that the Controller (Netors Investments Ltd) has changed its name to Varvelia Technologies Ltd. The Commissioner has verified through the companies' Registrar that there has been a name change and the company registration number remains the same (HE 346627).

Assessment

9. The Commissioner considers that the controller has complied with its obligations and brought the processing operations into compliance with the provisions of the Regulation. Considering the above, the Commissioner will not undertake any further action towards the Controller at this time and will close the investigation.

10. Based on Article 60(7) the Spain SA will inform the complainant about this Decision.

[REDACTED]
Commissioner for Personal
Data Protection



COMMISSIONER

Our ref.: 11.17.001.008.222

30 December 2022

Decision**Failure to Fully Comply to a Subject Access Request by Tarlun Limited**

1. A complaint was lodged with the French SA (CNIL Commission nationale de l'informatique et des libertés) against Tarlun Limited (the controller), whose main establishment is in Cyprus. Moreover, the complaint was subsequently transmitted to Office of the Commissioner for Personal Data Protection (Cyprus SA) on 25/9/2020, in line with Article 56 of the General Data Protection Regulation.
2. On the basis of the above, the Commissioner for Personal Data Protection (the Commissioner) is acting as the lead authority in this matter. In the course of the investigation, other EU countries were identified as being concerned by this case.

Description of the case

- 3.1. The complaint involves the controller's (Tarlun Limited) failure to comply with the complainant's access request (SAR) (article 15 of the GDPR) submitted to the controller, which operates the website www.funnycuistot.com.
- 3.2. In her complaint, the complainant stated that she was charged for subscription services to the benefit of the website www.funnycuistot.com, whereas she indicated that she did not remember having subscribed to this site. Following this, she exercised her right of access via email from [REDACTED] to support@funnycuistot.com on 31 August 2020 to identify what data was being held on her and where the data was collected from. Moreover, she accepted a partial refund, but she had not received an answer as regards the Subject Access Request. After not receiving the requested information, the DS lodged a complaint regarding the controller's failure to fulfill the request.

Investigation by Cyprus SA

4. In the framework of the investigation by the Cyprus SA, the following information was collected:
 - i. The complainant lodged a SAR via email with support@funnycuistot.com, exercising her right of access as a data subject under Article 15 of the GDPR on 31/08/2019 as well as an inquiry in relation to the subscription to the Website.

- ii. The controller wrongfully believed that the SAR was a request for a reimbursement for the subscription paid to the Website and that they already fulfilled it by refunding the complainant in September 2019.
- iii. Following the reimbursement of the complainant, the controller's Support Department was unable to recover and/or locate the complainant's SAR to reply and provide her with her personal data on time.
- iv. The controller became aware of the SAR on 15/12/2020, upon notification of the complaint by the Cyprus SA.
- v. As a result of reimbursement provided to the complainant, the controller continued to have a false impression that the SAR was satisfied until January 2022, when legal advisors were appointed, who clarified to the controller that the SAR was not satisfied.
- vi. Upon realising this, the controller on 24 March 2022 contacted the complainant and satisfied her SAR by providing her all the information she requested and further apologised for causing any inconvenience.
- vii. Moreover, the complainant confirmed the receipt of the above information and also stated: "*This indicates a fraudulent use of my information and credit card number from an IP address in the Rhône-Alpes region (whereas I am in the Grand Est region) but this is no longer within the scope of the right of access request. So, I have obtained satisfaction concerning my complaint and I thank you for it.*"
- viii. Furthermore, the controller took all necessary actions to avoid any recurrence of the above incident. Specifically, the controller commenced preparation of related policies and the appropriate technical and organizational measures for the compliance with the GDPR and also arranged for the conduction of further training/seminars of its personnel on the provisions of the GDPR and data protection in general.

Preliminary Decision

5. On 10 November 2022, the Commissioner issued a Preliminary Decision regarding the controller's failure to comply with the complainant's SAR. In the said Preliminary Decision the Commissioner concluded that Tarlun Limited had not complied with the complainant's request in a timely manner, thus there is a **violation of Article 12(3) GDPR** since the controller did not respond to her SAR within the one-month time limit.

6. The controller's legal representative responded on 15 December 2022, to the Preliminary Decision and stated, *inter alia*, that:

- i. The controller accepts the Commissioner's conclusion that there is a violation of Article 12(3) GDPR since the Company did not reply to the request made within the one-month time limit;
- ii. The controller notes that customer service employees wrongfully believed that the request made was a request for a reimbursement for the subscription paid to the website of the Company.
- iii. Following the incident, the controller emphasizes that GDPR training has been conducted for all its employees including all support managers.

7. In addition to the above, the controller's legal representative included the following mitigating factors to be taken into account by the Commissioner:

- i. There are no previous infringements committed by the controller,
- ii. the controller took every action and provided necessary information timely in order to cooperate with the Commissioner to remedy the incident as well as to help with the investigation and to mitigate the possible adverse effects of the incident,
- iii. the controller satisfied the access request as soon as the controller realized the incorrect handling of data subject request,
- iv. the incident in question involved only one data subject and the damage suffered by the data subject is minimal and
- v. no special categories of data were affected in this incident and to the extent the Company is concerned, any data received by the Company was provided by the complainant and the Company could not have known that the data was provided fraudulently (as claimed by the complainant).

Legal framework

8. Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject.

Pursuant to article 12(3) of the GDPR *The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.*

9. Article 15: Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) *the purposes of the processing;*
- (b) *the categories of personal data concerned;*
- (c) *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
- (d) *where possible, the envisaged period for which the personal data will be*

stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. *Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.*

3. *The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*

10. Article 58. Corrective Powers

2. *Each supervisory authority shall have all of the following corrective powers:*

...
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; ...

Preliminary Views of the Commissioner

11. After reviewing the information provided by the controller's legal representative, in their response to my Preliminary Decision, specifically the fact that the controller appreciates that there was a lack of appropriate attention to the complainant's request, I consider that the controller understands that the request could have been satisfied from the first instance if the support staff was properly trained in tackling GDPR requests in a timely manner.

12. Despite this, considering that the GDPR had been enforced for more than a year at the time of the complainant's first SAR, the controller should have had the appropriate measures in place for **at least** satisfying data subject rights set out in Articles 15 to 22 of the GDPR. Moreover, the complainant should have

received a valid response without delay to its first SAR, where he **clearly** requested to be informed of all his personal data which was processed by the controller at the time.

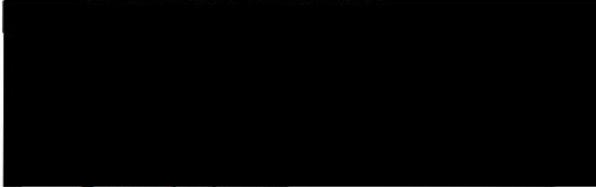
Decision

13. Having regard to all the above information, and based on the powers vested in me by **Articles 58 and 83 of Regulation (EU) 2016/679 and article 24(b) of National Law 125(I)/2018**, I conclude that there is an infringement by Tarlun Limited of Article 12(3) of the GDPR, since the controller has not complied with the complainant's request in a timely manner.

14. Moreover, following an infringement of Article 12(3) GDPR, as explained above, under the provisions of Article 83 of the GDPR, I take into account the following mitigating (1-3) and aggravating (4-6) factors:

1. That there is no previous violation by the controller of the GDPR 2016/679.
2. The controller satisfied the access request as soon as the mistake was realized
3. The measures taken after the incident to ensure that all staff is appropriately trained in handling GDPR matters.
4. The controller only became aware of the SAR after being notified of the complaint by my Office.
5. The complainant's request was not satisfied within the legal timeframe.
6. The lack of appropriate procedures and measures for handling data subject rights at the time of the request.

15. In view of the above and on the basis of the powers conferred on me by the provisions of subparagraph (b) of paragraph (2) of Article 58 of the GDPR, I have decided to issue a reprimand to Tarlun Limited for the infringement mentioned in paragraph 13 above. In the event of a recurrence of a similar infringement within 12 months from today, this Decision may be counted against the company.



Commissioner
For Personal Data Protection

From: [REDACTED] @dataprotection.gov.cy>
Sent: Πέμπτη, 5 Ιανουαρίου 2023 2:45 μμ
To: 'Privacy VulkanVegas'
Subject: Investigation of complaint under the General Data Protection Regulation (GDPR)

Ref: 11.17.001.010.084

Tel: 22818456

Fax: 22304565

January 5, 2023

Brivio Limited

privacy@vulkanvegas.com

Subject: Investigation of complaint under the General Data Protection Regulation (GDPR)

Following the instructions of the Commissioner of Personal Data Protection, I would like to refer to the complaint lodged in Austria and was thereafter received by the Office of the Commissioner for Personal Data Protection in Cyprus SA on behalf of [REDACTED] (the Data Subject - DS).

2.1 The DS, who is a registered user on the online casino "vulkanvegas.com", submitted his access request via email to privacy@vulkanvegas.com on 04 November 2021, requesting that Brivio Limited (the Controller) provide him with information regarding the transactions, account activities and other account data as is his legal right according to Article 15 of the GDPR. After not receiving a reply, the DS lodged a complaint regarding the Controller's failure to fulfill the request within the one-month period pursuant to the Article 12(3) and (4) of the GDPR.

2.2 Our Office contacted you using the email address mentioned in your website and requested your views on the matter raised by the DS. The company's Compliance Team replied and informed us that, the request to access had been made by an attorney on behalf of the DS and the email address with which the request had been made was not associated with the registered account of the latter. Moreover, the Attorney had not provided any documents to confirm that they were lawfully entitled to act on behalf of the DS. The request had not been satisfied, as it deemed invalid due to the fact that you had reasonable grounds to doubt the legality of the request.

2.3 In our response, you were informed that, according to the Article 12(6) of the GDPR, the Controller may request the provision of additional information necessary to confirm the identity of the DS, when the former has reasonable doubts concerning the identity of the natural person making the request. Also, it was noted that, if the controller does not take action on the request, the controller shall inform the DS at the latest within one month of receipt of the request of the reasons for not taking action (Article 12(4)). Nevertheless, the request was submitted in November 2021 and according to the DS, you did not receive any answer to their email within the one-month period.

2.4 Moreover, you admitted that no additional information was requested to assure that the attorney was entitled to represent the DS. However, it was your position that, after receiving the complaint, you requested a document that confirmed the Attorney's right to submit the access request on behalf of the DS. A power of attorney had been provided and the DS's access request had been satisfied the same day.

2.5 Furthermore, you informed our Office about the following corrective actions taken to improve your practices and to avoid similar cases in the future: the issue tracking software was implemented, internal procedures for handling data subject requests were amended and extra training for staff who regularly interact with individuals was conducted.

2.6 Our Office confirmed, by contacting the DS's representative, that the access request had indeed been satisfied.

3.1 Considering the fact that Brivio Limited eventually complied with the access request, the Commissioner is of the view that the mere delay appears to be a minor infringement which only slightly affects the DS's rights and freedoms.

3.2 After consideration of the significance of the infringement and your cooperation in the investigation process, the Commissioner considers that the investigation proceedings can be concluded as no further supervisory measure is necessary at this stage.

Yours sincerely,

[REDACTED]
for the Personal Data
Protection Commissioner



REPUBLIC OF CYPRUS



OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Ref. N.: 11.17.001.009.225

Tel. No.: 22818456

Fax No.: 22304565

Email: commissioner@dataprotection.gov.cy

SEND BY POST (DOUBLE REGISTER)

15 May, 2023

[REDACTED]

Crowd Tech Ltd

(c/o Data Protection Officer)

Decision Unsolicited calls and erasure request

Further to the exchange of communications between Cyprus SA (the Commissioner for Personal Data Protection) and Crowd Tech Limited concerning a complaint involving Trade360.com, we would like to bring to your attention the following assessment of the Commissioner.

Summary of the Case

2. A complaint was lodged on the 20th of November, 2020 in Poland against Athena Investments Dom Makerski S.A. ("the processor"). The complainant claimed that the processor processed his data without a legal basis, since he has never provided them with his phone or personal information, nor has he given them his consent for marketing calls. The complainant clarified that only contact with the processor was by telephone, and any request to delete his personal data, ended immediately the recorded conversation, so that the request could not be registered. He did not take any other steps to solve the situation with the processor.

2.1 The Polish Supervisory Authority contacted the processor and the processor answered that it had received the complainant's data from the company Crowd Tech Ltd ("the controller") on 31.08.2020. They processed the complainant's data (name, surname, telephone number and email address) on behalf of the controller. The legal basis for processing was Article 28 of Regulation 2016/679. The purpose was to present the services offered by the controller and they have called the complainant by phone on 01.09.2020 and 20.11.2020, informing him that they were acting on behalf of the controller. According with the processor, the complainant did not request deletion of his data, he simply stated that he was not interested in the services offered to him. They did not receive any written request from the complainant (in writing or by

an e-mail) addressed to the DPO. The processor presented to the Polish SA part of the processor's agreement with the controller, in support of its position. Then, the complaint was transmitted by the Polish SA to the Commissioner for Personal Data Protection (Cyprus SA), to be handled as a local case, since the controller is an investment company registered in Cyprus.

2.2 Before investigating the complaint, we asked clarifications from the Polish SA. The complainant (through the Polish SA) clarified that he was not a client of the controller, that the call was on his private phone number and that he exercised his rights towards the processor asking the erasure of his personal data from their database.

2.3 During the investigation of the complaint with the controller, the controller initially clarified the following, presenting relevant documentations to establish its positions:

- There was indeed a call between the processor and the complainant.
- The complainant was considered to be lead (potential client) as he never activated any trading account with the controller and thus no contractual relationship was established between them.
- His information was provided by the complainant, via online marketing/landing pages and banners to either a partner, affiliate or the company. During this process, leads may then share their information via their account registration through landing pages and banners. The aforementioned registration of the complainant occurred from a specific (given) IP address through a specific landing page via which the complainant accepts to receive further marketing calls. The complainant entered his information and submitted over a click of a button via the Polish Website as seen over a screenshot which the controller provided. According with the screenshot, the information of the complainant entered the system on the 28.8.2020 07:28 from a specific IP Address, using the trade360_pl site. The legal basis was consent, since any data subject can freely register over a landing page/website and submit registration details by a click of a button.
- The processor handles any GDPR-related data subject request by directly forwarding such request towards their DPO's email address. With respect to the case of the complainant, the processor notified the controller via email and the controller proceeded with unsubscribing the complainant from their records. The complainant was unsubscribed on 15.12.2020, i.e. the day of receipt of the request from processor. Relevant print screen was provided. Moreover, the controller provided us with their Clients Data Subjects Request Registry, confirming by this, the way they have handled the specific request.

2.4 The above clarifications were forwarded to the complainant through the Polish Authority. The complainant however insisted that he has never been a customer of the controller, wondering how the controller linked the click on the button to his phone number and his consent to phone contact, indicating that there was a very low probability that he used the button on August 28, 2020 at 7.28, because he was probably still asleep at this time, saying that he has reached out the processor asking to delete his personal data on 20 November 2021 and on 22 November 2021 he received a reply about their deletion, providing a photo of an email received by the

processor, and wandering if the processor has a copy of his request to delete his personal data, because his request was made later than indicated by the processor. He insisted to his complaint, because he thought the explanations provided as insufficient and the evidence provided as incomplete.

2.5.1 We informed the controller regarding the complainant's response and the controller replied that the complainant was categorized as per the company's internal procedure as a potential client since he entered his information over a landing page (Polish Website) and submitted his registration details. They had used the submitted data to contact him via their processor. This is the standard process followed for all leads. As far as the technical registration details they presented relevant screenshot indicating site of registration, date and time, and complainant's details. The complainant was not, at any time, categorized as a customer since he never proceeded further with registering a trading account. Actual identification of a person registering an account takes place in a Know-Your-Client (KYC) process and by that any successful request converts into an activated account and therefore prospective client turns into an actual client.

2.5.2 The deletion request reached them on 15.12.2020 through their processor. They executed the deletion request immediately and unsubscribed him from every means of communication. The request was handled within the thirty (30) days deadline to respond. Their business is based on real facts and not on guessworks, such as the one that the complainant is referring to (possibly sleeping). They also presented an unofficial translation of the phone call between the complainant and the processor, which indicated that the request for deletion was made by the complainant on 20.11.2020 and a year later, as it seems, the complainant returned with another email (20.11.2021) as arises from the communication between the processor and the complainant. Furthermore, the initial deletion request was made on 20.11.2020 to the processor and the complainant's second position is contradicting with his initial complaint, indicating 20.11.2020 as the date of the deletion request. Furthermore, the controller informed us that they have terminated their Agreement with the processor as from 31.08.2022.

2.6 We communicated the reply of the controller to the Polish Authority, which came back with the request to clarify the meaning of the document provided by the controller titled "AccountManagerDashboard_....", containing the complainant's name. According to their views, this document showed that the controller continues to process the complainant's personal data in the form of his first name, the name of the individual user number and locational data in the form of the place (country) where the complainant was present on 28 August 2020 at the time of use of the trade360.pl website.

2.7 In response to the above, the controller clarified that this document has been provided as evidence for registration details of the complainant. The information is stored into their systems and protected by the various security mechanisms according to ISO 27001 standard, continuous monitoring, etc. They also clarified that they are obliged by the MiFiD, MiFiR and national Law 87(I)/2017, as amended, (Article 17(6) and 17(7)), to keep records for clients or potential clients for at least 5 years and, where requested by the competent authority, up to seven years. Therefore, there is a

legal obligation which prevents the controller to delete the data. However, they have unsubscribed the data subject from their communication list and he has never been contacted again by any means. The controller furthermore stressed the fact that the complaint was filed the same date as the complainant's request for deletion

2.8 Having examined the controller's privacy policy, we also noticed that the data subject is informed that when they sign up/register to a trading account (both live/demo), the controller may collect personal data such as name, surname, date of birth, gender, phone, etc. The complainant at this case, was categorized by the controller as a potential client since, according with the evidence sent, he entered his information over a landing page and submitted his registration details. The complainant did not dispute the given I.P. address which was used to enter the information to the website.

Legal basis

3. Based on Article 12(3) of the GDPR the "The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request....".

3.1 According to Article 17(1)(c), the data subject can request from the controller the erasure of his personal data when the data subject objects to the processing pursuant to Article 21(2), i.e. for direct marketing purposes. The controller can refuse to delete data for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject (Article 17(3)(b)). However, "Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes." (Article 12(3) of the GDPR).

Assessment

4. From the facts of this case, it seems that the complainant received two calls from the processor. Then, the complainant requested verbally the deletion of his data on the 20.11.2020, i.e. the date of the second call received. The processor sent the request to the controller on the 15.12.2020 and the controller unsubscribed the complainant from all its communication list at the same day. From what the controller said, the complainant's data could not be totally deleted since there is a legal obligation which prevents the controller from deleting them. The controller is an investment company which is obliged by the MiFiD, MiFiR and national Law 87(I)/2017, to keep records for clients or potential clients for at least 5 years and, where requested by the competent authority, up to seven years. The complainant was classified as potential client when on the 28.8.2020 07:28 provided his information through the trade360_pl site. When registering to the website, a data subject provides his personal information, and as per the privacy policy, the data subject is informed that when they sign up/register to a trading account (both live/demo), the controller may collect personal data such as name, surname, date of birth, gender, phone, etc. Since the date of the complainant's deletion from the controller's communication list, the complainant did not receive any other marketing call.

Conclusion

5. Having in mind the results of the investigation, which showed that the complainants request was handled in due time and in respect of Article 12(3), 17(1)(c) and 21(3) of the GDPR, I find no reason to take any further actions or enforce any corrective power.

[REDACTED]

Commissioner
for Personal Data Protection

Final Decision

Case Register	474483
National file number	11.17.001.010.177
Controller	TechSolutions (CY) Group Ltd
Date	16.6.2023

TechSolutions (CY) Group Ltd
aml@techsolutions.group

Dear Sir,

Further to the exchange of communications between Cyprus SA (the Commissioner for Personal Data Protection) and TechSolutions (CY) Group Ltd (the controller) concerning a complaint involving a right of access request, we would like to bring to your attention the following assessment of the Commissioner.

Summary of the Case

2.1. [REDACTED] (the data subject) stated in his complaint, that he contacted the controller via his legal representative [REDACTED] ([REDACTED]) through email at aml@techsolutions.group on 16/3/2022, requesting that they provide information of all registration data related to him as is his legal right according to Article 15 of the GDPR. He also stated that he did not receive a reply to the above.

2.2. The Controller, TechSolutions (CY) Group Ltd, is registered in Cyprus, and therefore Cyprus SA is acting as the LSA for the complaint.

Cyprus SA investigation

3.1. Our Office contacted the controller and requested their views regarding their failure to satisfy the complainant's right of access request.

3.2. In their response, the controller informed us that the law firm representing the complainant had also made other enquiries regarding other clients which the controller had responded. As regards the request made on behalf of the complainant, it was unfortunately lost in the email chain with the law firm's email address. Despite this, as soon as they received a relevant complaint, they provided the complainant with the requested information on 25 October 2022 (please see a copy of the communication in the Relevant Documents section).

3.3. The complainant's representative confirmed the information received on 25 October 2022 and is satisfied.

Cyprus SA assessment

4. Considering the fact that the controller complied with the complainant's request immediately upon receiving our email, Cyprus SA is of the view that the

mere delay appears to be a minor infringement which only slightly affects the data subject's rights and freedoms.

5. After consideration of the significance of the infringement and the controller's cooperation in the investigation process, the Commissioner considers that the investigation proceedings can be concluded as no further supervisory measure is necessary at this stage.

6. The Commissioner reserves the right, in the event of any future complaints lodged by data subjects, to use all powers afforded to her by the GDPR and by national Law 125(I)/2018.

Commissioner
for Personal Data Protection
Cyprus

Ref: 11.17.001.009.097

26 January 2024

VIVERNO MARKETS LTD
(ex BDSwiss Holding PLC HE 300153)
Ioanni Stylianou 6
2nd floor, Office 202
2003 Nicosia
Cyprus
dpo@viverno.com

Subject: Decision: Right to erasure

I have been instructed to refer to our correspondence regarding the complaint of [REDACTED]
[REDACTED] and send you the Decision of the Commissioner.

[REDACTED]

for the Personal Data
Protection Commissioner

COMMISSIONER

Ref: 11.17.001.009.097

Decision

Right to erasure -- Viverno Markets Ltd

[REDACTED] (the complainant) has lodged a complaint with the State Commissioner for Data Protection North Rhine-Westphalia SA against *BDSwiss Holding PLC* (the Controller) that was received by the Office of the Commissioner for Personal Data Protection (Cyprus SA, henceforth the "Commissioner") according to the provisions of the cooperation and consistency procedures of the GDPR.

2. In line with Article 56 or the Regulation, the Commissioner is acting as the lead supervisory authority, as the Controller has its establishment in Cyprus.
3. It is noted that the Controller has changed its name to VIVERNO MARKETS LTD. The Commissioner has verified through the companies' Registrar that there has been a name change and the company registration number is the same (HE 300153).

Summary of the Complaint:

4. According to the complainant, the Controller did not delete his personal data despite repeated requests. In response to his requests by e-mail, he only received the message that his account had been closed, but his data was still stored. Unfortunately, he no longer has the corresponding e-mails.

Legal Framework

5.1. Article 12 of the GDPR states the following:

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
 - (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
 - (b) refuse to act on the request.The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.
7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

5.2. Article 17 of the GDPR states the following:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Investigation of the complaint

6. After contacting the Controller about the complaint, the Controller has informed the Commissioner the following:

The complainant has emailed the Controller asking for the closure of his account and the deletion of his personal data. The Controller closed the account and informed the complainant on the same date. On the same date, the complainant, emailed the Controller again, asking for the deletion of his personal data, in addition to the closure of the account. The Controller stated that it did not reply to his email due to the fact that the deletion of his data was not possible, due to the legal obligation to retain the data, and the complainant had already accepted the policy of the Controller. The legal obligation to retain the personal data stems from article 68.1 of the national Law for the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 to 2021, based on which the Controller has an obligation to maintain his data for a period of five (5) years after the end of the business relationship with the customer or after the date of an occasional transaction.

7. Following the above communication, the Controller has sent an email to the complainant informing him that his data cannot be deleted due to the above legal obligation and that his data will be retained for at least 5 years.

8. The Commissioner contacted the Controller again in order to clarify what is the exact retention period. It was clarified that the Controller has also an obligation to retain the data for 6 years from the end of the fiscal year, based on the tax legislation (the law on Certification and Collection of Tax Laws, Law 4/1978 (Section (30(2)).

9. Based on the above, the complainant is hereby informed that his data will be retained for a period of up to 6 years from the end of the fiscal year of the end of the business relationship with the Controller.

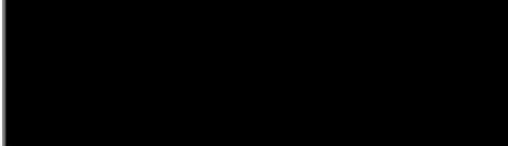
Assessment

10. The Controller was not obliged to delete the complainant's data, based on Article 17(3)(b) due to the fact it had a legal obligation to retain the data. However, the Controller has infringed the provisions of Article 12(4) because it did not reply to the complainant's 2nd email to provide him within one month, of the reasons for not taking action and about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

11. Based on Article 58(2)(b) the Commissioner issues a **reprimand** to the Controller for the infringement of Article 12(4).

Right of an effective remedy

12. Based on the Cyprus Constitution and *on The Establishment and Operation of the Administrative Court Law of 2015* (Law 131(I)/2015) the affected parties have the right to file an appeal against this Decision at the Cyprus Administrative Court, within 75 days from the day that the Decision was communicated to the affected party.



Commissioner for Personal
Data Protection
Cyprus
(Cyprus SA)

25 January 2024

Kypranoros 15, 1061 NICOSIA / P.O. Box 23378, 1682 NICOSIA. Tel.: +357 22818456, Fax:+357 22304565
E-mail: commissioner@dataprotection.gov.cy , Website: <https://www.dataprotection.gov.cy>



REPUBLIC OF CYPRUS



OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Our ref.: 11.17.001.009.100

8 February 2024

Decision

Failure to Fully Comply to an Erasure Request by Aylo Social LTD

A complaint was lodged with the Baden-Wurttemberg SA against MG Social LTD, recently rebranded as Aylo Social LTD (the controller), whose main establishment is in Cyprus. Moreover, the complaint was subsequently transmitted to the Office of the Commissioner for Personal Data Protection (Cyprus SA) on 2/3/2021, in line with Article 56 of the General Data Protection Regulation (GDPR).

2. On the basis of the above, the Commissioner for Personal Data Protection (the Commissioner) is acting as the lead authority in this matter. In the course of the investigation, other EU Data Protection Authorities were identified as being concerned by this case.

3. The complaint was filed against the website mydirtyhobby.de that provides pornographic content to its users, and is managed by the controller.

Description of the case

4.1. The complainant had requested the erasure of his account and relevant data on 2 separate emails sent on 25 June and 6 July 2020 to support@mydirtyhobby.com. Up until the day of his complaint, he claims that he never received a reply regarding his erasure request. He also confirmed that his account was still active and that he was still receiving promotional emails.

4.2. The Cyprus SA contacted the Controller on 23 August 2021, and requested their views on the matters raised by the complainant. In their response, they mentioned that the relevant staff member responded to the complainant in both instances, providing him with the necessary information to correctly initiate and complete the relevant procedure.

4.3. As it was determined from the communication provided by the controller, the support staff responded with the available options regarding deactivation of the complainant's account or deletion of the same, providing further information on what each option entails. Additionally, a link was provided at the end of the message to initiate the deletion procedure. The complainant took no relevant or further action regarding the instructions provided.

4.4. Furthermore, it was noted that the link provided in the message as above, leads to an online platform (Managemydata.eu), where the data subject is requested to provide an email address for verification.

4.5. According to the information the controller provided, when a valid request is received, a procedure is initiated via ManageMyData, which enables the verification the identity of the requester as the correct data subject, in order to avoid unauthorized disclosure or deletion.

5.1. On 13 June 2023, the Cyprus SA contacted the controller and requested additional clarification and documentation regarding the above. Specifically, the controller was asked to clarify, inter alia:

- i. Which are the *reasonable doubts* that justify the verification of the data subject identity following Art. 12(6) GDPR,
- ii. whether the complainant's erasure request had been fulfilled,
- iii. if the complainant was informed that no action would be made on the erasure request within one month of receipt of the request (Art. 12(4) GDPR) and
- iv. information regarding the platform ManageMyData.eu such as
 - a. Which entity is responsible for the development and/or management of the platform.
 - b. Where is the platform hosted and where are the relevant personal data stored.
 - c. How are visitors to the platform informed of the processing of their data as per Article 13 GDPR.

5.2. In their reply on 22 June 2023, the controller stated, inter alia, the following:

5.2.1. The step regarding the verification of the data subject email, was added in the process of data subject right handling, to avoid any malicious attempts taking into consideration the unique nature of the industry.

5.2.2. The complainant's erasure request was not fulfilled since he did not proceed with the verification of his email. In any case, they have manually initiated the procedure, to which the complainant must now respond by verifying himself as the account holder (no email verification will be required).

5.2.3. On whether they informed the data subject about the fact that they would not act on the request, the controller stated that:

"We have responded in time, but the matter was pending verification from the data subject. Additionally, we would also kindly like to remind you that, per ICO guidance, the time frame to respond starts upon receiving verification>ID or other information that establishes the identity of the requester/data subject or a third party that represents the same and authorized to act on their behalf. We acknowledged that the request was received, and we informed the user about the required process."

5.2.4. Regarding the use of the ManageMyData platform, the controller clarified that:

- i. it is not a third-party platform/service; it has been developed and is controlled by an internal entity within the group.
- ii. it is solely under the MindGeek group of companies, serving several products simultaneously. It has been set up as an internal platform to deal with GDPR-related requests.
- iii. The service is hosted on Azure Cloud Environment in North Europe, and the data is stored in the same.
- iv. Because this platform can be used by a variety of products/sites of the same group of companies, the privacy policy of the website a visitor arrives at ManageMyData from, is the one that is in effect.

Preliminary Views of the Commissioner

6. On 17 November 2023, I issued a Preliminary Decision regarding the controller's failure to notify the complainant of the erasure of his data. In the said Preliminary Decision, I concluded that:

6.1. In examining whether the verification process is excessive in violation of Article 12(2) GDPR:

6.1.1. It was noted that, in the controller's response, they did not ask for more information. The response offered an alternative option for deactivation but also provided, in the same response, the link required to complete the erasure request. By following the link, the data subject would only need to provide his email address, which was previously known to the controller, solely for verification purposes and no other information was requested.

6.1.2. Additionally, in reference to the EDPB guidelines 01/2022 on data subject rights - Right of access (para. 72): "*In practice, authentication procedures often exist and controllers do not need to introduce additional safeguards to prevent unauthorised access to services. In order to enable individuals to access the data contained in their accounts (such as an e-mail account, an account on social networks or online shops), controllers are most likely to request the logging through the login and password of the user to authenticate, which in such cases should be sufficient to identify a data subject.*"

6.1.3. Moreover, I deemed that implementing an additional step for verification purposes in order to prevent malicious attempts, is not considered excessive especially since no additional data is collected for this purpose. Additionally, implementing such a safeguard ensues that there is a balance between the risks for the rights and freedoms of natural persons, and the security of the processing throughout the process of handling data subject requests in accordance with Art. 32 GDPR.

6.1.4. Thus, using a mechanism to verify a data subject identity through his registered email address, can be considered an adequate justification for the

facilitation of data subjects' rights in compliance with Art. 12(2). This view is also enhanced taking into consideration the special categories processed pursuant to Article 9 GDPR, where the controller should take extra precautions to mitigate the risk of mistakenly sharing personal data with the wrong data subject.

6.2. In examining whether the controller informed the data subject about the fact that it would not act on the request in line with Art. 12(4) GDPR:

6.2.1. Despite the controller's response above in paragraph 5.2.3, I consider that the controller should have informed the data subject, within the timeframe set in Article 12(4), that they would not act on the erasure request for the reason that the data subject did not complete the verification process. Thus, there is a breach of Article 12(4) GDPR.

6.2.2. Additionally, as a consequence of the controller's inactivity to inform the data subject as above, I consider that there is also a violation of Article 17 GDPR since the data subject's account is still active.

6.3. As regards the use of the ManageMyData platform:

6.3.1. From an investigation of the platform, it is clear that the platform is used only for websites and/or products developed by the MindGeek group and its subsidiaries. Despite this, although the only visitors to the platform are data subjects who received the link by the controller, I consider that they should have at least provide information on the controller behind the website even if it is the same controller. Moreover, this is in breach of Article 13 GDPR.

6.3.2. Additionally, I consider that the process involving the use of the platform may constitute a structural flaw in the controller's process of granting data subject rights. Following this, I recommend that the controller reviews this process and ensure that it is more transparent and clearer towards the data subjects.

Controller's response to the Commissioner's Preliminary Decision

7. The controller responded on 14 December 2023 to my Preliminary Decision and stated, *inter alia*, that:

7.1. the complainant never responded, nor proceeded with any relevant actions, either on the Support email chain, or on the ManageMyData platform.

7.2. pursuant to the data subject's complaint to the DPA and the subsequent communication between the controller and the Cyprus SA, the deletion procedure was initiated by the controller on behalf of the complainant who was therefore invited to take the necessary steps to verify himself as the account holder, something the complainant has not realized up to that day.

7.3. according to EDPB Guidelines 01/2022 on data subject rights - Right of access (para.157), "...when the controller needs to communicate with the data subject due to the uncertainty regarding the identity of the person making the request there

may be a suspension in time until the controller has obtained the information needed from the data subject, provided the controller has asked for additional information without undue delay.”.

7.4. having invited the Data Subject (in multiple instances) to proceed with his request via the dedicated platform, and that both manually and proactively initiated the request on his behalf, the controller has shown clear intent to comply with the erasure request. As such, the case was not closed but suspended, until the necessary information for the verification of the Data Subject was obtained.

7.5. in a factually similar case, the Swedish Data Protection Authority (IMY) found that the controller “*had reasonable reason to doubt the identity of the complainant and thus request that the complainant submit additional such evidence, which the complainant did not respond to. Against this background, IMY considers that the company was not obligated to take any further measures due to the request*”.

7.6. regarding information provided to the data subjects who use MMD, it is noted that visitors (in any capacity) of a platform under the control of the Aylo group of companies do not usually receive a link via e-mail, like in this case. Instead, based on the fact that all relevant links to MMD (such as for GDPR deletion requests) are readily available in the respective privacy policy of each such website, where a user must navigate to in order to begin such process, they believe that Art. 13 GDPR requirements are fulfilled.

7.7. mitigating factors to be taken into consideration are, the unintentional nature and details of the incident, the fact that only a single data subject is concerned, the timely responses and willingness to cooperate – both with the data subject itself and with the Cyprus SA– and that no other, previous and/or similar cases have occurred involving Aylo Social Ltd.

Legal framework

8.1. Pursuant to Article 5(1)(c) of the GDPR “*Personal Data shall be:*

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

...

8.2. Pursuant to Article 12 of the GDPR:

...

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

...

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the

possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

..."

8.3. Pursuant to Article 13 of the GDPR:

"1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;*
- (b) the contact details of the data protection officer, where applicable;*
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
- (e) the recipients or categories of recipients of the personal data, if any;*
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.*

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*
- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;*
- (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*
- (d) the right to lodge a complaint with a supervisory authority;*

- (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information."

8.4. Pursuant to Article 17 of the GDPR:

"1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

..."

8.5. Pursuant to Article 58(2) GDPR, "each supervisory authority shall have all of the following corrective powers:

...(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
...(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
...(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;"

Final Views of the Commissioner

9. In addition to my assessments mentioned in my Preliminary Decision, the following are noted:

9.1. Although the complainant never responded to the controller's emails, nor proceeded with the relevant instructions, the controller should have informed the data subject that they would not act on the erasure request in line with Article 12(4).

9.2. The controller initiated the deletion procedure again by sending the same instructions via email to the complainant (see para. 7.2. above). The fact that the complainant did not proceed with the same procedure, proves that the use of the current structure of granting data subject rights needs to be reviewed and refined to cover all possible scenarios. Additionally, considering that the complainant's email is in fact verified, his request should have been satisfied by now without requiring any other action.

9.3. The case mentioned by the controller in paragraph 7.5 involved a request that came from an e-mail address other than the one linked to the relevant account, therefore justifying the controller's actions on requesting proof of identity. In the present case, however, the complainant sent the request through the same email that was linked to his account. Thus, no further identification was needed or justified.

9.4. As regards the use of the ManageMyData platform and the Article 13 requirements, it is be noted that MMD is accessed in 2 ways. Most of the times, relevant links to MMD are readily available in the respective privacy policy of each such website, where a user must navigate to in order to begin such process. The second method is via e-mail such as in the present case. In any case though, all visitors should be presented upon arrival with information regarding the owner/controller of the platform to comply with Article 13.

Decision

10. Having regard to all the above information, and based on the powers vested in me by Articles 58 and 83 of Regulation (EU) 2016/679 and article 24(b) of National Law 125(I)/2018, I conclude that there is an **infringement of Articles 12(4), 13 and 17 GDPR** on behalf of Aylo Social LTD for the reasons mentioned above.

11. Moreover, following an infringement of Article 12(4), 13 and 17 GDPR, as explained above, under the provisions of Article 83 of the GDPR, the following mitigating (1-3) and aggravating (4-6) factors are taken into account:

1. That there is no previous violation by the controller of the GDPR.
2. The controller's willingness to cooperate with the Cyprus SA and to improve the process of handling data subject requests.
3. A single data subject is concerned by the case
4. The complainant's erasure request is still unsatisfied
5. The complainant was not explicitly informed that his request was not satisfied.
6. The lack of appropriate procedures and measures for handling data subject rights at the time of the request.

12.1. In view of the above, I have decided to issue to Aylo Social LTD:

- a. **a reprimand** for the infringement of Article 12(4), and 13 on the basis of Article 58 (2)(b) GDPR and
- b. **an administrative fine of €1,500 (one thousand five hundred euro)** pursuant to Article 83 for the infringement of Article 17 on the basis of Article 58 (2)(i) GDPR.

12.2. In addition to the above I have decided to **order** Aylo Social LTD to:

- c. comply with the data subject's erasure request without any delay on the basis of Article 58 (2)(c) GDPR and
- d. bring processing operations into compliance on the basis of Article 58 (2)(d) GDPR, specifically:
 - i. Provide adequate information regarding the controller on the ManageMyData platform in line with Article 13 GDPR and
 - ii. Review the procedure for handling data subjects request and inform the Cyprus SA of relevant action within 2 months.

[REDACTED]
Commissioner
For Personal Data Protection
Cyprus



REPUBLIC OF CYPRUS



OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Ref. no.: 11.17.001.010.121

Decision

Demonstration of data subject's consent and provision of information relating to processing

1. A complaint was lodged with the Office of the Data Protection Ombudsman in Finland (Finland SA) against Naxex Invest Ltd (the Controller), whose establishment is in Cyprus. The complaint was subsequently transmitted to the Office of the Commissioner for Personal Data Protection (Cyprus SA) on the 22nd of June 2022, in line with Article 56 of the General Data Protection Regulation.
2. On the basis of the above, the Commissioner for Personal Data Protection (the Commissioner) is acting as the lead authority in this matter. In the course of the investigation, other EU countries, such as Finland SA, were identified as being concerned by this case.

Description of the case

3.1. According to the complaint, on the 15th of May 2020 the Complainant received a phone call from FXGM “about investing”. During the call, the Complainant requested to be informed about the collection and use of his data (his contact details) by FXGM. As he stated, he was informed that his contact details were collected via a Facebook-ad.

3.2. Following the call, on the same day, the Complainant submitted an access request via e-mail to FXGM, requesting, among others, the below:

1. information about the source used to collect his personal data (“where and how, (...) when”);
2. the categories of his personal data processed;
3. the purposes of the processing and the legal basis for the processing;
4. the recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries;
5. a copy of his personal data undergoing processing.

3.3. On August 13, 2020 FXGM informed the Complainant that his personal data including his contact details, were provided by Swarmiz (<https://www.swarmiz.com/>) on the 26th of April 2018. FXGM assured the Complainant, that his data has never been disclosed to third parties and provided to the Complainant with a copy of his personal data which were under processing (Name, Telephone Number, Email address, I.P. address). The Complainant was

informed that FXGM would proceed with the deletion of his personal data from its database.

3.4. On the same day, the Complainant stated *inter alia* that there was an inconsistency to FXGM's reply, that his clear consent was not shown and he requested a proof of it. FXGM declared in its response that "*Furthermore, we would like to hereby inform you that the Company is not responsible for the security or privacy of any information that you may have submitted on your own accord with any third parties. Therefore, you can contact Swarmiz (<https://www.swarmiz.com/>) directly for any further enquiries that you may have.*"

3.5. The Complainant doubted that he ever consented for the processing of his personal data.

3.6. The above-mentioned exchanged e-mails of the Complainant with the Controller were submitted to the Finland SA as an attachment to the complaint.

3.7. Upon receiving the complaint, on the 9th of March 2022, Finland SA asked the Controller for specific clarifications concerning the above-mentioned lodged complaint. The Controller has informed Finland SA, among others, the below:

1. the Complainant registered to a marketing campaign operated by Swarmiz SL;
2. the Complainant's data were provided to the Controller on the 26th April, 2018 as a result of his registration to Swarmiz SL's marketing campaign;
3. the Controller has satisfied Complainant's access request and his right to be forgotten;
4. the Controller has directed the Complainant to Swarmiz SL, in order to assist him with any further inquiries he may had.

Investigation by Cyprus SA

4.1. FXGM was at the time of the incident, a registered EU trademark exclusively used as a brand name of Depaho Ltd, a registered Cyprus Investment Firm regulated by the Cyprus Securities and Exchange Commission. Depaho Ltd is the previous name of the Controller. The Controller duly incorporated under Cyprus Law, with registration no. HE292004, is authorized and regulated by the Cyprus Securities and Exchange Commission as a Cyprus Investment Firm. Therefore, the Controller is authorized to offer certain online investment and ancillary services and activities on the basis of Law 87(I)/2017, under license number 161/11.

4.2. Cyprus SA contacted the Controller and requested its views on the matters raised by the Complainant. According to the Controller's responses (dated 31st of August 2022, 20th of October 2022 and 20th of February 2023):

1. The Controller was authorized to passport its services on a cross-border basis including Finland.
2. The Controller no longer provides services to retail clients, since November 3, 2021.
3. On the basis of a signed agreement dated 17th of December 2013, Internovus Ltd was providing marketing services to the Controller.

4. A GDPR agreement regarding the provision of the said services, was signed on 25th of May 2018 between the Controller and Internovus Ltd.
5. On the basis of the said agreement, marketing services would be provided only to potential clients who gave their consent to receive further information about the Controller. Individuals would give their consent to their personal data being shared with the Controller by registering to a marketing campaign.
6. Swarmiz SL was acting as a sub-affiliate of Internovus and it was providing online services to Finland. Therefore, Swarmiz SL was operating at the time, the marketing campaign which allowed interested individuals to register their details and express their interest and consent for their data to be shared with the Controller and to receive information about its services.
7. The Complainant's data were provided to the Controller on the 26th of April 2018 by Swarmiz SL, after he completed his registration on the marketing campaign run. As a result of the Complainant's registration, the Controller collected and stored his name, telephone number, email address and I.P. address.
8. There was only one telephone communication with the Complainant by the Controller on the 15th of May 2020. During the call, the Complainant exercised his right of access. On the same day, the Complainant submitted an access request via e-mail to the Controller's DPO.
9. On the 13th of August 2020, the Controller provided the Complainant with all the requested information. Taking into consideration that the Complainant had never registered to a trading account, the Controller proactively proceeded with the deletion of all his data. The Complainant was informed about his data deletion via e-mail, on the 13th of August 2020.
10. As the Controller stated, due to the Complainant data deletion, all the records indicating his consent were anonymized.
11. The Controller processed Complainant's data on the grounds of legitimate interest.
12. The purpose of the processing was limited to the Complainant's communication and information provision about its services.

As proofs of the above-mentioned, the Controller attached to its responses the below:

- the service Agreement between Depaho Ltd and Internovus Ltd signed on the 17th of December 2013;
- the GDPR data Processing Agreement between Depaho Ltd and Internovus Ltd signed on the 25th of May 2018;
- the "BON DE COMMANDE NoOI201821022018" between Internovus Ltd and Swarmiz SL, dated 21/02/2018;
- a screenshot of the Complainant's profile;
- the exchanged emails between the Controller and the Complainant regarding his access request.

Preliminary Decision

- 5.1. Taking into consideration all the explanations and information provided on behalf of the Controller, as mentioned above, on the 6th of October 2023, I issued a Preliminary Decision regarding the Controller's failure to demonstrate the Complainant's consent and the lawfulness of the data collection.

5.2. Before the submission of its views and positions regarding the preliminary decision, the Controller requested the opportunity to orally represent the case. On the 8th of October 2023, a hearing was held at the Cyprus SA's offices in the presence of the Managing Director, the Data Protection Officer and the Legal Consultant of the Controller.

5.3. On the 17th of November 2023, the Controller responded to the Preliminary Decision, and stated, *inter alia*, that:

1. Interested individuals would register on their own will and volition, in different online campaigns, operated by Internovus Ltd or its sub-affiliates, expressing their interest and providing their consent and instruction to be contacted and receive further information about the Controller, its services and registration to its platform. These individuals were identified and categorized internally by the Controller as potential clients. The Controller would not engage in any direct communication or process personal information prior to the potential clients registering their interest in the services and consenting to be contacted to receive further information.
2. The Controller only contacted potential clients who had successfully registered their interest and provided their consent to be contacted.

This statement includes the Complainant's case. The Complainant had demonstrated interest in the Controller's services and consented to be contacted. As the Controller states, the Complainant's consent can be demonstrated by comparing the data maintained in the Controller's system (which was provided to the Cyprus SA before in the Screenshot) with the exchanged e-mails between the Controller and Internovus Ltd concerning his access request (emails dated May 19th, 2020 and August 4th, 2020).

3. The Complainant's successful registration to the online campaign in turn created a potential client profile in the Controller's systems as depicted in the provided Screenshot, confirming the information submitted by the Complainant being his name, surname, telephone number, email address. In addition to that information, the Controller retained the Complainants registration time stamp, IP and online campaign to which he had registered to as depicted in the provided Screenshot as "*Attempt Time*" and "*Campaign*" respectively. Read in conjunction with the IP address, confirms and provides proof of Complainant's consent and instruction to be contacted by the Controller.
4. Cyprus Securities and Exchange Commission has stringent regulations on the promotion of investment firms' services. In adherence to these Applicable Laws¹, the Controller would only contact individuals who had successfully registered and have explicitly consented to the sharing of their

¹ L. 87(I)/2017 regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets, Directive 2014/65/EU on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, Regulation (EU) No 600/2014 on markets in financial instruments and amending Regulation (EU) No 648/2012, Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive

personal information showing an interest in the services provided by the Controller.

5. There was a telephone conversation with the Complainant on the 15th of May, 2020, during which the Controller provided him with the relevant information regarding the Controller and its services, as legally obligated under Applicable Laws (to provide potential clients with the information and relevant risk disclosures during the pre-contractual phase) and directed the Complainant to its website, where all pertinent details and information, including the Privacy Policy, were readily accessible in a durable medium. The Complainant exercised his right to access information during the call, which was subsequently followed up in writing. The Complainant never proceeded further to finalize his registration.
6. The Controller promptly acknowledged receipt of the Complainant's request to access his information. On the 13th of August, 2020, the Controller provided the Complainant with its official response; furnishing all information available in its records. Within the same response, the Controller informed the Complainant that "*it would at that time proceed with the "deletion of your personal data from our database"*". The Complainant did not, at any time, raise any objection or express discomfort regarding the Controller's notification to delete the specific collected information.
7. The Controller adheres to specific obligations governed by Applicable Laws (Law 87(I)/2017, Directive 2014/65/EU, Regulation (EU) No 600/2014, Commission Delegated Regulation (EU) 2017/565) regarding the collection, processing, and retention of personal data. It is noted that these requirements pertain specifically to the Controller's clients.
8. The Complainant's information submitted and shared with the Controller were limited only to his full name, email, telephone number and IP address. For the avoidance of any doubt, the Controller disclosed all information to the Complainant at the time of his request, as shown on the relevant correspondence.
9. It is the Controller's position that the legal basis and legal purpose for the collection and process of the Complainant's data was in accordance with the Applicable Laws and Articles 6 and 7 of the GDPR.
10. On the 13th of August, 2020, the Controller did respond to the Complainant's access request, providing him with all the available and relevant information it hid in its systems (as shown in the Screenshot).
11. The Controller has clarified in its response dated 17 November 2023, that despite proceeding with notifying the Complainant for the intention to delete his data, the Controller's DPO has retained the exchanged e-mails between the Controller and Internovus Ltd concerning the Complainant's access request (emails dated May 19th, 2020 and August 4th, 2020) within his internal records as part of the procedure of handling the request.
12. In relation to Article 6 of the GDPR, which sets out the legal basis under it is allowed personal data can be processed, **the Controller is of the opinion that it was acting in compliance with the provisions therein.**
 - o As per the Controller, the collection and processing of the Complainant's personal information was based on Article 6(1)(a), (b) and (f). The conditions of Article 7 in relation to consent are duly satisfied by the Complainant's registration attempt on the Controller's system as provided in the relevant Screenshot.

- Following the comment of the Cyprus SA that the information in the Screenshot does not link to the Complainant due to being anonymised, the Controller's DPO was able to find relevant correspondence regarding the Complainants request in its internal records (emails dated May 19th, 2020 and August 4th, 2020).
 - As evident in the said correspondence, the email subjects of both e-mails, labelled "CRM Lead 13071131," aligns with the Load ID specified in the provided Screenshot.
 - Additionally, both emails encompass the personal information held by the Controller in relation to the Complainant, which was also disclosed to the Complainant in the Controller's response to his request on the 13th of August, 2020.
 - Further, email dated 4th of August 2020 provides a report extracted from the Controller's system at the relevant time, presenting an overview of the Complainant's information within the Controller's system records. The "Serial ID" corresponds to the identifier presented in the Screenshot.
 - Both e-mails also evidence that the Controller maintained and maintains necessary records in place relating to Complainant's access request.
13. The Controller noted that the decision to proceed with the deletion was based on the following considerations:
- that the Complainant, on his own will and volition proceeded with the registration on the promotional campaign, expressing his interest to receive further information thus was categorised as a potential client;
 - that the Complainant never finalised his registration to become a client indicating that his interest ceased to exist;
 - that the Controller fully satisfied the Complainants request for access to his information;
 - the Controller's decision to proceed with anonymisation was done after proper notification to the Complainant was made and without receiving his opposition to the notification from his side; and
 - in any event, the Controller is of the opinion that the deletion would not and has not adversely affected in any way the Complainant's legal rights, specifically in this case, his right to privacy.
14. The Controller considered that since there was no lex specialis obligation to further retain the Complainant's information, the deletion of the Complainant's information was in accordance with the provisions of Preamble 39 of the GDPR.
15. The Controller, having considered that the Complainant was only a potential client that did not show further interest in its services after being contacted and has not finalised his registration further, considered that deletion of Complainant's information was justified under Article 5(1)(e) since the legal purpose for the collection and processing of the information ceased to exist.
16. In addition to the above and for the avoidance of any doubt, the Controller also considered that the deletion of the Complainant's personal information is also in compliance with Preamble 64 of the GDPR which states that "... *A controller should not retain personal data for the sole purpose of being able to react to potential requests.*" As provided in the Applicable Laws, the Controller's specific record keeping obligations is in relation to individuals

that are categorised as clients of the Controller. Considering that there is no specific reference to the retention of potential clients' records, the Controller treats such additionally in line with the GDPR provisions.

17. Therefore, in conclusion of all the above, it is the Controller's opinion that all the actions taken by the Controller in relation to the collection, process and anonymization of Complainant's specific data submitted at the time were made in absence of any bad faith or effort to elude from any of its legal obligations and the Controller genuinely believes to have been acting in accordance with the provisions of the GDPR.

As proofs of the above-mentioned, the Controller attached to its response the below:

- the service Agreement between Depaho Ltd and Internovus Ltd signed on the 17th of December 2013;
- the GDPR data Processing Agreement between Depaho Ltd and Internovus Ltd signed on the 25th of May 2018;
- the "BON DE COMMANDE NoOI201821022018" between Internovus Ltd and Swarmiz SL, dated 21/02/2018;
- a screenshot of the Complainant's profile;
- the exchanged e-mails between the Controller and Internovus Ltd concerning the Complainant's access request (emails dated May 19th, 2020 and August 4th, 2020);
- the exchanged emails between the Controller and the Complainant regarding his access request.

Legal framework

6.1. Recital 39 of the Preamble:

"Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be

established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."

6.2. Recital 42 of the Preamble:

"Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment"

6.3. Recital 47 of the Preamble:

"(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. (...) At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. (...) The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

6.4. Recital 61 of the Preamble:

"(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided."

6.5. Recital 64 of the Preamble:

"The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests."

6.6. Article 6: Lawfulness of processing

Pursuant to Article 6(1) of the GDPR,

"1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;*
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

6.7. Article 7: Conditions for consent

According to Article 7(1) of the GDPR, *"Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."*

6.8. Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

According to Article 12(1) of the GDPR, *"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means."*

6.9. Article 13: Information to be provided where personal data are collected from the data subject

"1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;*

- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (d) the right to lodge a complaint with a supervisory authority;
- (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information."

6.10. Article 14: Information to be provided where personal data have not been obtained from the data subject

"1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- (d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
- (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (e) the right to lodge a complaint with a supervisory authority;
- (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
- (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

- (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
- (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2."

6.11. Article 15: Right of access by the data subject

"1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;

- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 - (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (f) the right to lodge a complaint with a supervisory authority;
 - (g) where the personal data are not collected from the data subject, any available information as to their source;
 - (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others"

6.12. Pursuant to Article 58(2) GDPR, "each supervisory authority shall have all of the following corrective powers:

(...) (b)to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation"

6.13. L. 87(I)/2017 regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets

- "client means any natural or legal person to whom an IF provides investment or ancillary services;"
- Article 17 of the L. 87(I)/2017:
"(7)(a) - "The records provided for in subsection (6) shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders."
- Article 25 of the L. 87(I)/2017:
"25.-(1) A CIF must, act honestly, fairly and professionally when providing investment services, or, where appropriate, ancillary services, to clients, in accordance with the best interests of its clients, and comply, in particular, with the principles set out in section 26.
(...)"

(3) CIFs must ensure that:

(a) all information, including marketing communications, addressed to clients or potential clients are fair, clear and not misleading, and

(b) marketing communications are clearly identifiable as such."

(4)(a) A CIF ensures that appropriate information is provided in good time to clients or potential clients with regard to the CIF and its services, the financial instruments and proposed investment strategies, execution venues and all costs and related charges, and that, such information includes the following:

(i) when investment advice is provided, the CIF must, in good time before it provides investment advice, inform the client:

(A) whether or not the advice is provided on an independent basis; and
(B) whether the advice is based on a broad or on a more restricted analysis of different types of financial instruments and, in particular, whether the range is limited to financial instruments issued or provided by entities having close links with the CIF or any other legal or economic relationships, such as contractual relationships, so close as to pose a risk of impairing the independent basis of the advice provided;

(C) whether the CIF will provide the client with a periodic assessment of the suitability of the financial instruments recommended to that client;

(ii) the information on financial instruments and proposed investment strategies must include appropriate guidance on and warnings of the risks associated with investments in those instruments or in respect of particular investment strategies and must state whether the financial instrument is intended for retail or professional clients, taking account of the identified target market in accordance with subsection (2);

(iii) the information on all costs and associated charges must include information relating to both investment services and ancillary services, including the cost of advice, where relevant, the cost of the financial instrument recommended or marketed to the client and how the client may pay for it, also encompassing any third-party payments.

(b) The CIF ensures that the information about all costs and charges, including costs and charges in connection with the investment service and the financial instrument, which are not caused by the occurrence of underlying market risk, shall be aggregated to allow the client to understand the overall cost as well as the cumulative effect on return of the investment, and if the client so requests, an itemised breakdown of the costs shall be provided. Where applicable, such information shall be provided to the client on a regular basis, at least annually, during the life of the investment."

6.14. DIRECTIVE 2014/65/EU on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU

- Article 16 of the Directive 2014/65/EU:

"(6) An investment firm shall arrange for records to be kept of all services, activities and transactions undertaken by it which shall be sufficient to enable the competent authority to fulfil its supervisory tasks and to perform the enforcement actions under this Directive, Regulation (EU) No 600/2014, Directive 2014/57/EU and Regulation (EU) No 596/2014, and in particular to ascertain that the investment firm has complied with all obligations including those with respect to clients or potential clients and to the integrity of the market.

(7) Records shall include the recording of telephone conversations or electronic communications relating to, at least, transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of client orders (...)

(...) The records kept in accordance with this paragraph shall be provided to the client involved upon request and shall be kept for a period of five years and, where requested by the competent authority, for a period of up to seven years"

6.15. REGULATION (EU) No 600/2014 on markets in financial instruments and amending Regulation (EU) No 648/2012:

- Article 25(1) of the Regulation (EU) No 600/2014:

"Investment firms shall keep at the disposal of the competent authority, for five years, the relevant data relating to all orders and all transactions in financial instruments which they have carried out, whether on own account or on behalf of a client. In the case of transactions carried out on behalf of clients, the records shall contain all the information and details of the identity of the client, and the information required under Directive 2005/60/EC of the European Parliament and of the Council (1). ESMA may request access to that information in accordance with the procedure and under the conditions set out in Article 35 of Regulation (EU) No 1095/2010."

6.16. Commission Delegated Regulation (EU) 2017/565 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive:

- Article 72 (2):

"Investment firms shall keep at least the records identified in Annex I to this Regulation depending upon the nature of their activities.

The list of records identified in Annex I to this Regulation is without prejudice to any other recordkeeping obligations arising from other legislation."

Views of the Commissioner

7.1. After examining the facts and the information provided by the Complainant and the Controller, and taking into consideration the comments from the concerned Supervisory Authorities, I would like to mention the below.

7.2. Naxex Invest Ltd as the legal entity, who determined the purposes and means of the processing is considered as the Controller. The Complainant as the natural person whose personal data were being processed is considered as the data subject.

7.3. According to the Controller, the Complainant registered his details and express his interest and consent to receive information about the Controller's services. During the data collection the Complainant was provided with some initial information about the purpose of the processing. Furthermore, during the call on the 15th of May 2020, the Controller provided some additional information regarding the data processing to the Complainant. It was explained to the

Complainant that his data were provided to the Controller as a result of his registration to a marketing campaign regarding the Controller. It was moreover explained that the Complainant consented for his details sharing in order to receive information about the Controller and its services. According to the Controller, during the call the Complainant was provided with the relevant information regarding the company and its services, and was directed to its website, where all pertinent details and information, including the Privacy Policy, were readily accessible in a durable medium.

7.4. Following the call and upon the receipt of the Complainant's request of access (dd May 15th, 2020), the Controller has provided the relevant information concerning the data processing on the 13th of August 2020. With the said e-mails:

- The Controller informed the Complainant about the collection, the recipients of his data and provided him with a copy of his personal data undergoing processing.
- The Controller informed the Complainant that it would proceed with the deletion of his personal data from its database.
- The Controller referred the Complainant to Swarmiz SL's for further details concerning the ad.

7.5. Based on the facts, the collected personal data were used only for communication of the Controller's services with the Complainant. The Complainant was informed about the processing of his personal data at the time of the collection and at the time of the Controller's first communication. The Controller provided the Complainant with additional information about his data processing by its reply to the submitted access request.

7.6. Taking into consideration the above, the Controller provided to the Complainant information about his data processing at the time of the collection and at the first communication (in accordance with Articles 12, 13 and 14 of the GDPR). Moreover, it responded to his access request within the specified time frame (as defined in Article 12 of the GDPR) and provided the information the Complainant has requested in his access request.

7.7. As the Controller stated, the Complainant's data were collected and further processed (storage and use) based on consent and on the grounds of legitimate interest. It was also stated that the processing was necessary in order the Controller to take steps at the request of the data subject prior to entering into a contract.

7.8. The Complainant has disputed that he previously consented to receive information about the Controller. In order to investigate the validity of the Complainant's consent, the Controller was instructed to send to my Office any relevant documentation has in its possession. As a proof of the data subject's consent, the Controller initially sent to my Office a Screenshot of the Complainant's profile. The Screenshot shows a Table which contains the below information:

- Lead ID: 13071131
- Label: FXGM_FIN
- Attempt time: 26-Apr-18 7:25:51 AM

- Campaign: Swarmiz_Trainees_Finland [26FEB2018] [14622]
- Serial Id: 1156290
- IP address: [REDACTED]
- Pseudonymized first name, last name, phone, e-mail of the Complainant.

7.9. The Controller stated that the above-mentioned information was anonymized due to the deletion of the Complainant's data. As it was clarified to the Controller, anonymous registration doesn't prove the Complainant's consent. Therefore, before the issuance of the Preliminary Decision, the Controller was requested to provide further documentation in order to prove the Complainant's consent. On the 20th of February 2023, the Controller stated that has already provided my Office with all the available information and supporting documents. Consequently, taking into consideration that the Complainant has never requested his data deletion and repeatedly asked for a proof of his consent, in my preliminary decision I found that the Controller did not have a plausible reason to proceed with the deletion of his data and I concluded that the Controller had failed to demonstrate the Complainant's consent and the lawfulness of the data collection.

7.10. According to the Controller's response to my Preliminary Decision, the Complainant's registration and consent provision can be demonstrated by the information mentioned in the previous paragraphs. In order to prove that, the Controller sent to my Office two additional emails. Those emails were exchanged in 2020 (May 19th, 2020 and August 4th, 2020) between the Controllers and Internovus Ltd employees regarding the Complainant's access request. The e-mail dated August 4th, 2020 includes a report extracted from the Controllers system at the relevant time, presenting an overview of the Complainant's information. The report includes among others the below:

7.11. Reading the above-mentioned details in comparison with the information given in the Screenshot of the Complainant's profile, the Controller is of the opinion that it can be concluded that the information which categorized as anonymous relates to the Complainant and indicates his registration.

7.12. It is important to highlight that, according to Recital 26 of the Preamble of the GDPR, anonymous information is information which does not relate to an identified or identifiable natural person. Consequently, the data regarding the Complainant cannot be considered and characterized as anonymous (as the Controller initially stated), since the Complainant can be indirectly identified.

7.13. Moreover, according to Guidelines 05/2020 on consent under Regulation 2016/679, Article 7(1) of the GDPR clearly determines the explicit obligation of the controller to demonstrate the data subject's consent. According to the same Article, the burden of proof of the consent validity is on the controller. Recital 42 of the Preamble of the GDPR states: "*Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data*

subject has given consent to the processing operation." As per the Guidelines 05/2020, Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations. The controllers should have enough data to show a link to the processing (to show consent was obtained) but they shouldn't be collecting any more information than necessary.

7.14. The GDPR does not prescribe exactly how the Controller must prove its compliance with the GDPR. In any case, the Controller must be able to prove that the data subject has given consent to the processing operation.

7.15. Taking into consideration all the above, I am of the opinion that the provided information and the documentation indicates up to a point the Complainant's registration to the marketing campaign. However, the provided information (including all the additional documentation) doesn't demonstrate compliance with the main elements of the consent requirement as stipulated in Articles 4(11) and 7 of GDPR (freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her).

7.16. Concerning the processing of the Complainant's personal data for direct marketing purposes, I consider that processing for direct marketing purposes may be regarded as carried out for the Controller's legitimate interest.

7.17. Regarding the deletion of the Complainant's data, I am of the opinion that the Controller did not act in a way that negatively affect the Complainant's rights and freedoms. In any case, I find important to highlight that controllers have an obligation to stop the processing actions concerned and to delete data that was processed on the basis of consent once that consent is withdrawn, in the event that no other purpose exists justifying the continued retention. The completion of the examination of pending requests before any deletion and the provision of accurate and comprehensive information are deemed necessary.

Conclusion

8. Having regard to all the above information, and based on the powers vested in me by **Articles 58 and 83 of Regulation (EU) 2016/679 and article 24(b) of National Law 125(I)/2018**, I conclude that there is an infringement of **Articles 6 and 7 GDPR** on behalf of Naxex Invest Ltd for the reasons mentioned above.

9. Under the provisions of Article 83 of the GDPR, I take into account the following mitigating (1-6) and aggravating (7) factors:

1. The Controller no longer provides services to retail clients.
2. There is no previous violation of the GDPR by the Controller.
3. The categories of personal data affected by the infringement.
4. The cooperation of the Controller with the supervisory authority.
5. The negligent character of the infringement.
6. The level of the damage the Complainant suffered.
7. The inability of the Controller to prove that all conditions for valid explicit consent were met.

10. In view of the above and on the basis of the powers conferred on me by the provisions of subparagraph (b) of paragraph (2) of Article 58 of the GDPR, I have decided to **issue a Reprimand** to Naxex Invest Ltd for the infringement mentioned in paragraph 8 above.

[REDACTED]
Commissioner
For Personal Data Protection
Cyprus

28th of March 2024



REPUBLIC OF CYPRUS



OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Ref. no.: 11.17.001.011.004, 12.10.001.011.006.004.066

Decision

Unauthorised processing of customers' personal data

1. A complaint was lodged with the President of Personal Data Protection Office in Poland (Poland SA) against Briju 1920 Limited (Company). The Company's head office is located in Cyprus and it operates as a plant in Poland. Consequently, on the 28th of December 2022 the complaint was subsequently transmitted to the Office of the Commissioner for Personal Data Protection (Cyprus SA), in line with Article 56 of the General Data Protection Regulation.

2. On the basis of the above, the Commissioner for Personal Data Protection (the Commissioner) is acting as the lead authority in this matter.

Description of the Case

3. According to the Complainant (Data Subject), on the 2nd of December 2022 she made an online purchase from Briju 1920 Limited (Company). On the same day, she received an e-mail from a third party who informed her about unauthorized access to her personal data due to the fact that the Company had never "*withdrawn the relevant data processing authorisations*". In the e-mail was mentioned that, the e-mail's sender had access to 7000 customers' personal data, such as their name, surname, address, telephone number, e-mail address and method/form of payment.

4. On the 5th of December 2022 the Company sent an e-mail with its official position on the above-mentioned incident. In the said e-mail, the Company's director informed its customers that all Company's security systems have been checked and appropriate technical and organizational protection measures have been implemented. The Company moreover confirmed that its databases are fully protected and any attempts of unauthorised access to data are and will continue to be effectively thwarted and provided the contact details of the Company's Data Protection Officer to the customers.

5. Afterwards the Data Subject called the helpline of the Company. As she mentioned, it turned out that she was not the only person to receive the above-mentioned e-mail. Since the provided explanations didn't satisfy her, on the 7th of December 2022, she requested information about the reasons that caused the breach and expressed, in written, her fear and stress for a future cyber-attack. Following her e-mail, the Company assured her once more for its databases' safety, informed her that any unauthorized

access was effectively thwarted and that the breach was already notified to the Commissioner's Office.

6. In the complaint, the Data Subject asked for an imposition of a fine to the Company and for her personal data erasure from the Company's database. The Data Subject attached to her complaint the e-mails dd 2/12/22, 5/12/22, 7/12/22.

Investigation by Cyprus SA

7. On the 6th of December 2022, the Company submitted the relevant Reporting Form in order to notify Cyprus SA about the above-mentioned incident (Data Breach Notification).

8. Cyprus SA informed the Company for the complaint submission and addressed questions to the Company in order to further investigate the reported incident (e-mails dd 16/1/23, 21/4/23, 13/10/23, 19/1/24).

9. According to the Company's submitted Data Breach Notification (dd 6/12/22):

- a) The email's sender sent an email to 100 of the Company's online customers, claiming/informing them that he has unauthorized access to their personal data. As he claimed, he was working for the Company but he retained access to the customers' data even after his leaving from the Company.
- b) The Company became aware of the incident on the 2nd of December 2022, when one of the data subjects who received the said email messaged the Company.
- c) As the Company explained, it is collecting the customers' personal data for the implementation of their orders. The e-mail addresses of the customers were downloaded from the Company's online store database. E-mail addresses were processed by the Company on the ground of Article 6(1)(b) of the General Regulation of Personal Data Protection (EU) 2016/679 (GDPR).
- d) The email's sender (Ex-employee) was processing the customers' data on behalf of the Company for the period he was working at the Company.
- e) As the Company clarified, the actual fraud email was sent to 100 customers even if the Ex-employee had claimed that he retained access to 7000 customers' personal data.
- f) The Company declared that even if the Ex-employee did retain some access to customers' information post leaving the Company, as he claimed, he should not have disclosed and/or communicated with the data subjects as this breaches any confidentiality clauses and/or NDAs and/or DPAs which formed part of his employment contract with the Company and which remain in force after an employee leaves the Company.
- g) The Company has introduced additional organisation and technical measures, to ensure access is granted and/or retained only to those who explicitly work and/or are involved with the Company for the said purposes and to avoid any such future incident from reoccurring in the future. The Company had further ensured that any access the Ex-employee had has been reclaimed.

10. As per the additional information which was provided by the Company (dd 3/2/23, 6/2/23, 16/5/23 and 1/2/23):

- a) The Ex-employee was still engaged by the Company on the date of the incident under the contract dated 15/11/2022. Therefore, the Ex-employee had authorized access to the data of the Company's customers at the time the incident occurred. On the 3rd of December 2022 the Company blocked any access the Ex-employee had at its systems (including the Company's platform). His contract with the Company was officially terminated on the 9th of December 2022.
- b) There was no reason at the time for the Company to be suspicious about its employees' intentions.
- c) Upon becoming aware of this incident, the Company proceeded with the below actions:
 - 1. On the 3rd of December 2022 the Company blocked any access the Ex-employee had at its systems (including the Company's platform). Therefore, his last logged in to the Company's system was on the 2nd of December 2023. The Ex-employee's access to the Company's platform was blocked by deleting his account (along with his login credentials).
 - 2. The remaining employees with access to the Company's platform were instructed to immediately change their login credentials.
 - 3. On the 9th of December 2022, the Company proceeded with an official termination of the Ex-employee's contract.
 - 4. The Company informed the recipients (customers affected by the incident) about the incident and requested them to permanently delete the correspondence that they fraudulently received.
- d) The DS erasure request was satisfied. It was noted that no personal data is kept by the Company, other than the invoices and receipts issued, based on her transactions and/or purchases. As per applicable law, the Company cannot delete those invoices/receipts. The DS has been informed adequately of this (via e-mail dd 3/2/2023). According to the additional information provided by the Company on the 1st of February 2024:
 - 1. Art. 86(1) of the Tax Ordinance (Act of August 29, 1997, Journal of Laws 2023.2383) obliges taxpayers to keep tax books and related documents until the limitation period for the tax liability expires, unless tax laws otherwise provide. These types of documents include VAT registers, accounting evidence such as sales and purchase invoices, internal documents, correction invoices, correction notes, accounting notes, records of fixed assets, inventory documents (physical inventory), etc.
Moreover, Art 70(1) of the Tax Ordinance states that the tax liability expires after 5 years, counting from the end of the calendar year in which the tax payment deadline expired.
 - 2. Art. 47 section 3c of the Act on the Social Insurance System (Act of October 13, 1998 on the Social Insurance System, Journal of Laws No. 2023.1230) states that copies of settlement declarations and personal monthly reports as well as documents correcting these documents, has to be kept for a period of 5 years from the date their transmission. This deadline applies to ZUS declarations submitted from January 1, 2012.

As proofs of the above-mentioned, the Company attached to its responses the below:

- the Contract dated 15/11/2022 between the Company and the Ex-employee and the Statement dated 15/11/2022;
- its Privacy Policy;
- an excel sheet representing the dates of the incidents,
- the e-mail dd 31/1/23 sent by Support Przelewy24.pl confirming that the ex-employee has the status "removed";
- a letter from the Director of PayPro S.A (dated 10/05/2023) and a Letter from the Company's Director (dated 16/5/23) confirming the last date of access of the Ex-employee and the deletion of his account;
- the e-mail dated 5/12/22 which was sent to the Company's customers affected by the incident and the email dd 3/2/23 sent to the Complainant.

Legal framework

11. Based on Article 5 of the GDPR,

"1. Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

12. According to Article 17 of the GDPR,

"1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*
- (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).*

(...)

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;*
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);*
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or*
- (e) for the establishment, exercise or defence of legal claims."*

Cyprus SA assessment

13. According to the provided information and the relevant Contract between the Ex-employee and the Company, the Ex-employee had legitimate access to the customers' email addresses for the time period he was working for the Company. On the basis of the Contract between the Ex-employee and the Company, at the time the incident occurred the Ex-employee was still working for the Company. It was then very difficult for the Company to take prior measures in order to prevent the reported incident and ensure appropriate security of the personal data, including protection against unauthorized processing by its employees.

14. According to the complaint, the Reporting Form and the evidences of the present case, the Ex-employee didn't use any other personal data of the customers besides their e-mail address; even though he claimed that he had access to their name, surname,

address, telephone number, e-mail address and method/form of payment. Therefore, there is no proof that the Ex-employee used in a fraud manner any other data except the customers' e-mails.

15. Concerning the Data Subject's erasure request no personal data is kept by the Company, other than the invoices and receipts issued based on her transactions and/or purchases. As it is explained above the issued receipts and invoices must be kept for compliance with a legal obligation of the Company.

Conclusion

16. Having regard to all the above information, based on the powers vested in me by Articles 58 and 83 of Regulation (EU) 2016/679 and article 24(b) of National Law 125(I)/2018 and taking into consideration that:

- a) no special categories of personal data were affected;
- b) data subjects were informed about the incident;
- c) at the time the incident occurred the Ex-employee was still working for the Company;
- d) the Ex-employee's access was immediately blocked;
- e) the contract signed by the Ex-employee included clauses which determine that he was authorized to process customers' personal data only to the extend and the purpose which was provided by the Company;

I conclude that no corrective powers shall be implemented to the Company. Taking into account the present case's individual circumstances and features (as mentioned above) I consider that the imposition of a fine is not proportionate since no violation on behalf of the Company was found.

17. In order to prevent such incidents in the future, I suggest to the Company to implement the below:

- a) constant control of the actions of employees;
- b) withdrawing certain forms of access from employees who have signaled their intention to quit or implementing access logs so that unwanted access can be logged and flagged.



12th of April 2024

Commissioner
For Personal Data Protection
Cyprus

A60 - Final Decision

Case Register	407627
National file number	11.17.001.010.089
Controller	Wargaming Group Limited
Date	18/7/2024

Wargaming Group Limited
privacy@wargaming.net

Dear Sir,

Further to the exchange of communications between the Commissioner for Personal Data Protection and Wargaming Group Limited (the controller) concerning a complaint involving a right of access request, we would like to bring to your attention the following assessment of the Commissioner.

Description of the Case

1. The complainant lodged a complaint with the Office for Personal Data Protection in the Czech Republic, and was thereafter received by the Office of the Commissioner for Personal Data Protection (Cyprus SA). The complaint involves the controller's failure to comply with the DS access request (SAR) (article 15 of the GDPR) submitted to the controller.
2. In his complaint the complainant mentioned that, when he requested information under Article 15 of the GDPR, the controller asked him to provide a telephone number to proceed with the request. In his response, the complainant claimed that he did not own a mobile phone and that the company could meet his request for access without providing any new information.

Investigation by Cyprus SA

3.1. The Commissioner engaged with the controller and following the exchange of several communications in relation to the subject matter of the complaint, the following information was gathered:

3.2. The controller stated that in the context of Article 12(6) GDPR and in order to maintain increased protection, security and control of their customers/users' data, 2-factor-authentication (2FA) is applied.

3.3. Moreover, the controller considered the additional telephone number requirement to be legitimate in cases where users request access under Article 15 of the GDPR and/or to change the email address linked to the user's account.

4.1. In relation to the above, our Office noted that the intention of the controller to request additional identification information is to protect any unauthorised disclosure. However, as stated in recital 64, the controller should not retain personal data for the sole purpose of being able to respond to potential requests. Therefore, it was determined that collecting a telephone number solely to satisfy the data subject's rights is excessive, regardless of when the data are collected.

4.2. Following this, the controller was requested to review the process of satisfying users' rights, without requiring data that had not already been collected at the time of registration. In their response, the controller stated that since 28/09/2023, they had revised the process of satisfying

users' rights without requiring data that had not already been collected at the time of registration, e.g., the collection of the telephone number is no longer required to satisfy users' rights except through the data already collected, such as email address.

4.3. The controller also confirmed that, on 28/12/2023 the complainant made another request for access by logging in to his account and was satisfied on 10/01/2024.

4.4. Our office requested from the complaint-receiving CSA (CZ SA) to confirm with the complainant that his request was indeed satisfied. According to the CZ SA the information was sent to the complainant on 13/3/2024 by email and on 26/03/2024 by post but received no answer so far. However, since the controller provided satisfactory proof of the access request satisfaction, no more evidence is required.

Commissioner's conclusion

In view of the above, considering that

- i. the Controller's purpose was to protect any unauthorised disclosure,
- ii. the Controller did not intend to bring harm to any data subject,
- iii. the Controller cooperated fully during the investigation and
- iv. the data subject's access request was eventually satisfied

the Commissioner considers that this case can be closed and there is no need for any corrective measures.

Cyprus SA