REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Our ref.: 11.17.001.011.218
11.17.001.012.012

4 September 2024

Decision

Investigation of complaints against the company Senira Limited under the General Data Protection Regulation (GDPR)

I refer to the investigation of two complaints against the company SENIRA LIMITED (hereinafter, the "Controller"), which operates the website www.nicelocal.com (hereinafter, the "website").

Description of the complaints

2.1. The first complaint was lodged in Germany, and is related to the Controller's failure to respond to a data subject request to erase their personal data. More specifically, the complaint concerns an entry published on the website www.nicelocal.com.de. The said entry contains personal data about the complainant (complainant 1) running a clothing tailoring service as a natural person (https://nicelocal.com.de/sachsen-anhalt/utility_service/n_design_nancy_beer/), and was published without the complainant's knowledge and against her will.

2.2. Complainant 1 contacted the Controller on 22/08/2023, by sending an email to the email addresses legal@nicelocal.com and content@nicelocal.com, requesting the immediate deletion of her personal data, as her legal right to erasure under Article 17 of the GDPR. On 11/09/2023 the complainant repeated her request by sending an email to privacy@nicelocal.com, which is the email address provided by the Controller to the public for matters related to personal data protection.

2.3. On 12/10/2023, complainant 1 informed the Supervisory Authority in Germany that she received no feedback from the Controller. Moreover, she claimed that the option "Request Removal of Content" which is available on the homepage of the website was not working.

3.1. The second complaint was lodged in Poland. The complainant (complainant 2) is a natural person, with a sole proprietorship under the name: [redacted]

[redacted] According to complainant 2, a profile of his business was created in the website nicelocal.co.pl, containing his name, photos of premises (most likely taken from google maps) and unverified reviews. The profile [redacted] was created without his consent or knowledge.

3.2. On 21/06/2023, complainant 2 requested the deletion of the aforementioned profile from the website (via content@nicelocal.com) and erasure of all the data contained therein. On the same day, he received an automated message informing him that his request was in progress. Despite the above, the entire profile remained, and only photos of the premises were removed. Also, the complainant claims that the following false information was contained in the profile: "Unfortunately, this place has been closed", which worked to his detriment as a businessman.

3.3. On 9/12/2023 complainant 2 repeated his request and received again the same automated massage, without however any success, since the relevant profile and all his personal data remained in the website.

4. On the basis of the Registrar of Companies in Cyprus, the Controller is registered in Cyprus, under registration no. HE 429529, and the address stated at the Registrar of Companies is Floor 3&4 M. KYPRIANOU HOUSE, Gladstonos, 116, 3032, Lemesos, Cyprus. On the basis of the above, the Commissioner for Personal Data Protection in Cyprus (hereinafter, the "Commissioner") is acting as the lead authority in this matter.

Investigation by the Commissioner

5.1. On 30/11/2023 the Commissioner's Office contacted the Controller as regards to the first complaint, requesting the latter's views and position on the same, the reason why the automated option "Request Removal of Content" was not working, and where was the personal data collected from and what is the legal basis and purpose for the relevant processing.

5.2. In its reply, dated 20/12/2023, the Controller stated the following:

i. They use a specially designed software to handle requests of this type received via email at privacy@nicelocal.com and legal@nicelocal.com.

ii. The option "Request Removal of Content" is placed at the bottom of each page and their team process requests after receiving them through a feedback form. They confirm that the said form works as expected.

iii. Data regarding the business "N/Design Nancy Beer" were collected from an open public source, namely Google. The Controller stated that the ground of processing is the fact that data comes from a publicly available source. Moreover, they stated that the data in question includes no special categories of data, stands for the public interest and helps business to grow by obtaining new clients on the web.

iv. Upon receipt of the Commissioner's letter, the Controller initiated a thorough investigation into the matter. They carefully reviewed the evidence provided, and they confirmed that they deleted the webpage https://en.nicelocal.com.de/sachsen-anhalt/utility_service/n_design_nancy_beer/.

v. The controller informed the Commissioner that they would carry out additional work to analyze the causes of what happened with the software algorithms.

5.3. The Commissioner confirmed through a relevant check that the personal data of complainant 1 had been deleted. Notwithstanding the above, the Commissioner considered that further information was required as regards to the way the system that handles the relevant request operates, and the safeguards and actions/measure taken by the controller in line with the GDPR. Moreover, the controller in its response failed to provide a valid legal basis, and the relevant purpose as to the processing of personal data. To that end, and as part of the investigation of the first complaint, a second letter was sent to the controller on 05/01/2024.

5.4. The controller failed to respond within the deadline specified in the aforementioned letter of the Commissioner, i.e. by the 25th of January 2024. In the meantime, the Commissioner's Office received the second complaint described in paragraphs 3.1.-3.3. above.

5.5. On 05/02/2024 the Commissioner sent another letter to the Controller, requesting a respond to the letter dated 05/01/2024, informing them about the second complaint and requesting their views on the same.

5.6. The Controller once again missed the deadline, and a reminder was sent by the Commissioner's Office on 06/03/2024. The Controller's response dated 07/03/2024 was the following:

"First and foremost, I would like to express my utmost respect as we value the importance of maintaining a positive business environment, and we strive to ensure that our client's and user's data are under protection and control.

Therefore, we appreciate your bringing this matter to our attention so that we may address it appropriately.

We use a specially designed software to handle these types of requests. Unfortunately, this case shows that we still have room for an improvement.

Upon receipt of your letter, we initiated a thorough investigation into the matter. We have carefully reviewed the evidence provided, and we can confirm that at the date of this letter the webpage [redacted] *has been deleted.*
We will carry out additional work to analyze the causes of what happened with the software algorithms and assure you that we are always attentive to the rights of personal data subjects in accordance with the requirements of the GDPR."

5.7. On 12 April 2024, the Commissioner issued a Preliminary Decision against the Controller where the following was identified:

(a) infringement of the Article 12(3) of the GDPR since the controller did not satisfy the complainants' requests for erasure of their personal data, in accordance with the provisions of the said Article.

(b) infringement of the Article 31 of the GDPR, since it failed to cooperate with the Commissioner's Office and provide the requested information.

5.8. Following the above, the Commissioner ordered the Controller to respond to the Commissioner's Office letter dated 05/01/2024, and particularly to provide the information requested in paragraphs 3.2. and 4.4.

5.9. In their response, on 12 May 2024, the controller stated the following:

i. The relevant processing is lawful for the purposes of the legitimate interests pursued by the Controller in accordance with Article 6(1)(f) GDPR. This is confirmed by the fact that the information collected regarding the business, including name, address or contact information, was manifestly made public by the data subjects on public sources such as Google.

ii. In the case of the first complaint, the erasure request was processed by the automated system, however, an error occurred as a result of which the said page was not deleted. In any case, the relevant information was removed on 19 December 2023, after the notification from the Commissioner's Office.

iii. In the case of the second complaint, the relevant information was removed on 6 March 2024, again after the notification from the Commissioner's Office.

iv. The Controller uses an automatic inquiry processing system that processes incoming inquiries, analyzes their content and takes appropriate actions, sending automatic notifications of the actions taken. If the system is unable to recognize a request, it sends it to the processing center for manual processing.

Legal framework

6.1. According to article 4 of the GDPR:

"(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
(2) *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*
(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;".

6.2. Article 5 of the GDPR sets out the principles according to which personal data shall be processed:

"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').".

6.3. For a processing to be lawful, one of the following conditions set out in article 6 of the GDPR must be applied:

"(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.".

6.4. Paragraphs 2 and 3 of article 12, which is related to the obligations of a controller as regards to data subject requests under Articles 15 to 22, state the following:

"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.".*

6.5. The right of a data subject to erasure ('right to be forgotten') is stipulated in Article 17 of the GDPR.

6.6. Article 24(1) of the GDPR is related to the responsibility of the controller to implement appropriate technical and organisational measures to safeguard the rights and freedoms of data subjects, in accordance with the GPDR:

"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, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.".

6.7. Further to the above, article 32(1) states the following:

"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: ...".

6.8. Article 31 of the GDPR refers to the obligation of a controller to cooperate with the Supervisory Authority, upon a relevant request:

"The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of

its tasks."

6.9. Pursuant to Article 58(1) of the GDPR, the Commissioner has, amongst other, the investigative powers:

"(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;".

6.10. Moreover, according to Article 58(2) the Commissioner has the following corrective powers:

"(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c) to order the 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 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 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 restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(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;
(j) to order the suspension of data flows to a recipient in a third country or to an international organization."

6.11. As regards to the administrative fines that may be imposed by the Commissioner, Article 83(2)-(6) states the following:

"(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.

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:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) 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.".

Commissioner's Views

7.1. The Controller's website provides information about organizations/ professionals/ individuals providing services, along with clients' reviews. The GDPR applies only to natural persons and does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons. However, information in relation to one-person companies may constitute personal data where it allows the identification of a natural person. The same applies to all personal data relating to natural persons in the course of a professional activity, such as the employees of a company/organization, business email addresses which reveals the individual's name etc.

7.2. The complaints in question concern information published in the Controller's website, referring to the complainants as individuals providing services. To that end, this information constitutes personal data and the GDPR applies. The collection and publication of the said information constitutes processing activities.

7.3. The Controller did not take actions within the one-month period specified by the GDPR as regard to the complainants' request made under article 17 of the GDPR, for erasure of the aforementioned information, in violation of the provisions

of the Article 12(3). The complainants' requests had been fulfilled by the Controller, only after the intervention of my Office.

7.4. It should be noted that the aforementioned complaints were not the first time my Office dealt with the Controller, since it had previously investigated a similar complaint against the Controller regarding an unsatisfied erasure request, lodged by an Italian citizen.

7.5. According to the information provided by the Controller as regard to the investigation of all the above complaints, all emails sent to legal@nicelocal.com, privacy@nicelocal.com and content@nicelocal.com are collected in a single cluster for their primary processing by a special AI system that recognizes the type of request and passes it on to the correspondent specialist for further consideration. As it seems, the failure of the Controller to respond/fulfil the relevant requests, is a result of a system failure to properly recognize the requests and pass them to the relevant department.

7.6.1. Due to the repeated nature of the Controller's failure to fulfill data subjects' requests for erasure of their personal data, my Office proceeded with further investigation of the matter. To that end, it requested additional information as regards to the operation of the said system and the technical measures taken in this regard (paragraph 3.2 of letter dated 5/1/2024). Despite my Office repeated efforts, the Controller failed to provide a response in this regard. It should be noted that the relevant questions were deliberately ignored by the Controller, since in their latest response, the Controller addressed other matters, avoiding to refer to the above.

7.6.2. The information requested in paragraph 3.2. of the aforementioned letter is of outmost importance. The absence of clear and specific information, as regard to the operation of the automated system used to recognise and forward the said requests to the relevant department to be handled, prevents proper evaluation of the risks involved. Systematic failures of the system in question, which consequently lead to mishandling of data subjects' requests, may be considered as failure of the Controller to facilitate the exercise of data subject rights under Articles 15 to 22, in violation of article 12(2) GDPR. Moreover, possible lack of appropriate technical measures implemented by the Controller to safeguard data subject's rights and freedoms, may constitute violation of article 24(1) and 32(1) GDPR.

7.6.3. In the Preliminary Decision, I ordered the controller to provide the information requested by my office in paragraphs 3.2. and 4.4. of the email dated 5/1/2024. Although a response was provided for paragraph 4.4., which referred to the legal basis of the processing, it was noted that the controller did not provide:
(a) detailed description of how this system operates,

(b) safeguards applied by the company to ensure that the system will properly handle all the requests,
(c) actions/measures taken by the company after our Office brought to its attention, through the first complaint, that the system does not works as it should,
(d) whether the company carried out a data processing impact assessment in accordance with article 35 of GDPR
as requested in paragraph 3.2. if the above email. The lack of response to these constitutes a violation of Article 31 GDPR.

7.7. As regards the legal basis for the collection and publication of personal data of individuals in the websites, the controller considered that the processing is lawful the achievement of the legitimate interests pursued by them. In that end, considering the following facts:

i. the personal data in question were originally made public on widely known public sources by the complainants themselves,
ii. the purpose of the processing of the data by the controller has not changed from the original purpose, i.e. the publication of the contact details of their businesses,
iii. there is no indication that the controller has used the data for any purposes other than the initial purpose and
iv. no harm can come to the data subjects from the further publication of their data since they were already published on a public source.

I find that the relevant processing is lawful and necessary for the purposes of the legitimate interests pursued by the controller as per paragraph 1(f) of Article 6 GDPR. This is enhanced by considering the exception for allowing the processing of special categories of personal data as it is stated in paragraph 2(e) Article 9 GDPR:
[the prohibition in] "Paragraph 1 shall not apply if one of the following applies: …

(e) processing relates to personal data which are manifestly made public by the data subject…"

According to the GDPR special categories of data are to be held at a higher level of protection, therefore the above exception can be proportionally applied on the processing of non-special categories of personal data.

7.8. In addition to the above, the controller is still obligated to *"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"* as per Article 12 GDPR. Moreover, the privacy policy on the controller's website should also include the sources used to collect the personal data in compliance with Article 14 GDPR and the transparency principle.

7.9. The failure of the Controller to respond all the Commissioner's questions and provide sufficient and conclusive information as explained above in paragraphs 7.6.1, 7.6.2 and 7.6.3, is in violation of article 31 GDPR.

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 12(3) and 31 GDPR** on behalf of Senira Limited for the reasons mentioned above.

9. Moreover, following an infringement of Article 12(3) and 31 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) The complainants' erasure requests were all satisfied eventually
(2) No harm has occurred to the data subjects from the further processing.
(3) The relevant processing does not involve sensitive data.
(4) The increasing number of complaints regarding the unsatisfied erasure requests
(5) The lack of appropriate procedures and measures for handling data subject rights.
(6) The lack of response to the Order issued on the Preliminary Decision

10. In view of the above, I have decided to issue to Senira Limited:

a. **a reprimand** for the infringement of Article 12(3) GDPR and
b. **an administrative fine of €3,000 (three thousand euro)** pursuant to Article 83 for the infringement of Article 31 on the basis of Article 58 (2)(i) GDPR.

11. In addition to the above I have decided to order Senira Limited to bring processing operations into compliance on the basis of Article 58 (2)(d) GDPR, specifically review the procedure for handling data subjects request so that no data subject requests are lost and inform the Commissioner's Office of relevant action within 2 months.

Commissioner
For Personal Data Protection

REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Our ref.: 11.17.001.012.009

22 January 2025

Decision

Failure to Fully Comply to an Erasure Request by Freedom Finance Europe Ltd

A complaint was lodged with the Federal Commissioner for Data Protection and Freedom of Information in Germany (Berlin SA) against Freedom Finance Europe 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), 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 failure to comply with the complainant's erasure request (article 17 of the GDPR) submitted to Freedom Finance Germany TT GmbH in Germany which is a subsidiary of the Controller.

3.2. The complainant stated that he registered an investment account through the controller's subsidiary in Germany on 30/9/2022. Moreover, on 1/11/2022, he sent an email to info@ffineu.eu and he requested the cancelation of his account, the erasure of his data and to stop receiving any advertising emails from the controller.

3.3. The complainant received a reply the same day from a customer support specialist, who informed him that he would need to log into his account for identification and to proceed with the closure of his account.

3.4. In his response the complainant demanded the deletion of his account without the need to log into his account.

3.5. According to the complainant, he did not receive another reply regarding his erasure request and his account was not deleted since he was still receiving relevant emails.

15, Kypranoros street, 1061 Nicosia / P.O.Box. 23378, 1682 Nicosia - Cyprus, Tel. +357 22818456, Fax +357 22304565
E-mail: commissioner@dataprotection.gov.cy, Website: http://www.dataprotection.gov.cy

Investigation by Cyprus SA

4.1. The Commissioner's Office contacted the Controller on 29/1/2024, and requested their views on the matter raised by the complainant as also proof that the complainant's personal data had been deleted.

4.2. In their responses, the controller mentioned, among others, the following:

i. The complainant expressly agreed to be bound by the provisions of the General Terms of Business (TOBs), including conditions laid out in the Annexes and any other relevant Addendums and all documents in Business Policies and Regulations located on the FFEU website.
ii. During the onboarding process, the complainant accepted the data protection and processing policy provided for in the Data Protection Notice.
iii. According to Section 8 of the Data Protection Notice, considering the general limitation period stipulated by laws of the Republic of Cyprus and in the absence of specific regulatory or contractual requirements their baseline retention period for the personal data is 7 years.
iv. Pursuant to section 37.2 of the TOBs, being in effect on 01/11/2022 – the date of the complainant`s request to cancel his account with the controller and to erase his data, the Client was obliged to terminate the contractual relationship with the Company first by following the steps set out in the TOBs, such as by giving an Instruction to close the Account in the Member Area section of the controller's website.
v. The complainant was notified of the account closure procedure via e-mail on the same day, 01/11/2022, as he requested. It was explained to the complainant that the personal data, meaning e-mail address for the regular e-mail notifications from the Controller, will be deleted once his account is closed.
vi. The complainant's account was closed on 01.02.2024, and a notification e-mail was sent to the complainant, including the information relating to GDPR on the retention of personal data for 7 years.

Preliminary Views of the Commissioner

5. On 25 October 2024, 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:

5.1. The complainant had requested that his account was closed and that his personal data are erased. After receiving a reply from the controller explaining that he must go through the identification process through the Member Area section of the controller's website, the complainant refused to follow the steps and sent another email explaining that his erasure request should be satisfied without following any other steps. The controller did not send any other responses. It is also noted that the controller proceeded with the closure of the complainant's account and notified him accordingly, though this was done after my Office first contacted the controller regarding the complaint.

5.2. In examining whether the verification process is excessive in violation of Article 12(2) GDPR:

5.2.1. In reference to the EDPB guidelines 01/2022 on data subject rights - Right of access (para. 73): "*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.*"

5.2.2. Moreover, implementing an additional step for verification and/or identification 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.

5.2.3. Thus, using a mechanism to verify a data subject identity through his registered member account, can be considered an adequate justification for the facilitation of data subjects' rights in compliance with Art. 12(2).

5.3. 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:

5.3.1. Although the controller replied on the same day to the erasure request, they did not reply to the second email where the complainant clearly stated that he considered his erasure request valid without the need for verification.

5.3.2. Moreover, we consider that the controller should have informed the complainant, within the timeframe set in Article 12(4), that they would not act on the erasure request for the reason that the complainant did not complete the verification process. Thus, there is a breach of Article 12(4) GDPR.

Controller's response to the Commissioner's Preliminary Decision

6. The controller responded on 6 November 2024 to my Preliminary Decision and stated, inter alia, that:

i. Their response to the complainant's request was both comprehensive and clear, providing instructions to follow by logging into his account to complete the identification process.
ii. The fact that their request for the complainant to complete the identification process was neither excessive nor unreasonable, affirms that their actions were well-justified and fully aligned with GDPR requirements and relevant guidelines.
iii. The complainant's subsequent request ("Request 2") did not substantially differ from Request 1. Given that the information has already been provided

comprehensively and timely in response to Request 1, there was neither a valid nor reasonable basis to issue a duplicate response to duplicative request. As such, non-provision of another identical response to a duplicative request does not constitute an abuse of the complainant's rights, but rather ensures efficient handling of inquiries.

iv. In matters involving "duplicative requests," it is essential to maintain a balance of interests. Once the complainant has received a comprehensive and thorough response to their initial request, any further duplicative inquiries should not serve as grounds for any alleged infringement. Failing to address this matter appropriately may result in an unjust situation where the submission of numerous identical requests could exploit the process as a whole, ultimately leading to an abuse of the data controller's rights and resources.

Legal framework

7.1. Article 12 of the GDPR states that:

"...

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.

..."

7.2. Article 17 GDPR: Right to erasure ('right to be forgotten')

"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).
…"

7.3. 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;
…(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

8. In addition to my assessments mentioned in my Preliminary Decision, the following are noted:

8.1. The controller's response provided clear instructions for the complainant to follow in order to close the account. As mentioned in section 5.2 above, the controller justifiably requests from the data subjects to follow this procedure so as to verify their identity and avoid wrongful disclosure or erasure of data, even by mistake. However, in the controller's response, it was not clear whether the complainant was obligated to follow this procedure or if there was an alternative way of satisfying his request. Hence the second request in which the complainant demanded again the erasure of his data without following the said procedure.

8.2. The controller, keeping in mind that the complainant would not follow the procedure, should have made it clear to the complainant that his request would not be satisfied, in line with Article 12(4) GDPR. More specifically, the first response to the request could have included a statement informing the data subject that his request would not be satisfied if the relevant procedure is not followed. Alternatively, the controller could have placed a mechanism to detect when a data subject's request is not satisfied from not following the procedure.

8.3. The fact that controller did not show any intention of not satisfying the complainant's request and proceeded with the erasure of the said data as soon as they received an email from my Office, is also taken into account.

Decision

9. 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 Freedom Finance Europe Ltd of Article 12(4) of the GDPR, for the reasons mentioned above.

10.1. 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 Freedom Finance Europe Ltd for the infringement mentioned above. In the event of a recurrence of a similar infringement within 12 months from today, this Decision may be counted against the company.

10.2. In addition to the above I have decided to **order** Freedom Finance Europe Ltd to review the information provided to the data subjects while exercising their rights (as explained in paragraph 8.2 above) and inform my Office within 1 month.

Commissioner
For Personal Data Protection

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA PROTECTION

Final Decision

Our ref. 11.17.001.008.042

12 January 2021

Data Protection Officer
SEA CHEFS CRUISES LTD
P.O. Box 59605
4011 Limassol, Cyprus

Dear Madam,

We refer to the complaint lodged in Germany against the company Sea Chefs Cruises Ltd (the controller), which was subsequently transmitted to the Commissioner for Personal Data Protection (Cyprus SA) and following the investigation of the case, we hereby inform you on the decision of the Commissioner.

A. Case description

The company's main activity is the provision of seafarer recruitment and placement services on cruise ships. Sea Chefs Cruises Ltd owns/manages the following companies: sea chefs River Cruises Ltd, sea chefs River Management Ltd, Ocean Spa Ltd, sea chefs Holding AG, sea chefs Cruises Worldwide GmbH, sea chefs Human Resources Services GmbH, sea chefs Cruise Management GmbH, sea chefs Malta Ltd, sea chefs Cruise Services GmbH, sea chefs Human Resources Services GmbH/Branch office Hamburg (jointly referred to as "the Company").

In the framework of its activities the company is held to comply with its legal obligations to conform with relevant laws, regulations and international conventions which makes it obligatory for the company to hold and process health-related data of employees and namely the Maritime Labour Convention, MLC 2006, International Labour Organisation, International Convention on Standards of Training, Certification and Watchkeeping for Seafarers 1978, as amended ("STCW") International Management Code for the Safe Operation of Ships and for Pollution, Prevention (International Safety Management (ISM) CODE), Guidelines on the medical examinations of seafarers, International Labour Organisation (ILO), International Maritime Organisation, Merchant Shipping Act (Cap. 234)/ Flag State Requirements of Malta, Merchant Shipping CH. 268 / Flag State Requirements of Bahamas and the Collective Bargaining Agreement.

The obligation includes the mandatory medical examinations for issuance of the Fit-For-Duty certificates.

Prior to beginning work on a ship, the company requests from employees to sign a general *Authorisation* for the release of medical records in order to have access to their medical records to

be able to assist the employees with medical care, to arrange any associated travel and to handle any medical claim, **in the event of a medical incident taking place onboard**.

Namely the "Authorisation for release of medical records" provides multiple purposes inter alia (1) the authorisation given to any doctor, pharmacist, insurance company etc. to disclose to Sea Chefs Cruises Ltd all health information and medical records […] (2) consent given to any other company or any other doctor […] who is in possession of medical/health data to allow Sea Chefs Cruises Ltd free access to those data (3) consent to the ability of the Company to ask questions and discuss the medical information [...] (4) consent to transfer or disclose medical data to local or foreigh Authorities an/or Agents etc. when it is provided by law or collective agreements or according to the terms of the employment [...].

Under the section "*Purpose of the authorisation for release of medical records*" of the Privacy notice (issue date 15-03-2019) the following is provided:

"*The Company needs to have your Authorisation for release of Medical Records, attached below, signed by you in order to be able to have access to your medical records. <u>This will only be necessary</u> in the event of a medical incident taking place onboard and for enabling the Company to manage your medical care and any associated medical claims timely and effectively.*

You have the right to refuse signing the Authorisation. However, in such a case please note that we will not be in the position to offer you employment since we will not be able to abide by our collective bargaining agreement obligations, offer you medical treatment when necessary, confirm you are fit for duty to safeguard your personal health and safety and to reduce risks to other crew members and for the safe operation of the ship."

The complainant, who works for the company, considers that such *Authorisation* is breach of the rules provided under the General Data Protection Regulation (GDPR).

B. Explanations provided by Sea Chefs Cruises Ltd

In the framework of the investigation by Cyprus SA, Sea Chefs Cruises Ltd provided the following information on 12.05.2020:

The company prepared and made available to its staff (data subjects) a Privacy Notice for the purpose, inter alia, of transparent communication and information about the personal data held in the company (including special categories of data), the purpose of their collection and processing, their rights regarding personal data, the legal basis for their collection, the administrative and technical protection measures applied, their retention period, etc.

The personal data collected from the data subjects is necessary for the execution of the work [contact] and the observance of the obligations of the company as an employer arising from its contractual obligations, from the relevant legal framework and for safeguarding the legitimate interests of the company. The relevant laws, regulations, international conventions and related contracts that render mandatory the collection and processing of health-related data by the controller are laid down in a separate list [attachment 1].

The need to provide an Authorisation for Release of Medical Records arose from the fact that the doctors/practitioners on board and the doctors at the medical centers where crew members are

transported for treatment, refuse to release the medical data to the company without the consent of the crew member. It is clarified that most doctors on board are employed by the clients of Sea Chefs Cruises Ltd, who are the ship-owning companies (outsourcing). Some doctors/practitioners work as free-lancers and in a few cases the doctors are employed by Sea Chefs Cruises Ltd.

Due to incomplete and/or insufficient relevant medical data provided by employees, the company is constantly exposed to the following risks:
1. Exposure the crew member and his health to danger, during his repatriation after illness or accident. The responsibility for the safe repatriation of each patient (employee) is assigned to the employer and not to the ship's doctor after disembarkation from the ship. In addition, post-repatriation recovery supervision is still the responsibility of the employer.
2. Failure to properly inform the family of each crew member (next of kin), after illness or accident. Informing the family is a contractual obligation under the Collective Bargaining Agreement .
3. Inability to properly defend a legal case in the event of legal proceedings.
4. Refusal of Maritime Insurance (P&I Club) to pay compensation.
5. Charging the company with the payment of Sickness Compensation for up to 130 days due to failure to submit relevant and sufficient medical data.

Several times, the company engaged discussions with its customers (mostly Germans) to find a solution to the release of medical records without much result. German customers continuously allege that in the industry all companies seek the consent of their employees to collect their medical data. If the company chose a different approach, the customers are afraid that the company would have a problem with employees and would constantly receive complaints and resignations. Some customers threatened to terminate their cooperation if the company did not provide this option.

Initially the Authorisation was a separate document and was given to the crew member when he or she needed medical care, off board, due to illness or after an accident. However, it was difficult and sometimes impossible to ask the crew member to sign the Authorisation at the time of a health problem or the accident. Therefore, the company decided to collect the Privacy Notice (general Authorisation) in advance, upon commencement of the employment, together with the Privacy Statement. If no medical incident or injury takes place and no medical claims are made against the Company, there will be no requirement to access medical records of the employees.

In order to assess whether the processing of employee's health related data by Sea chefs Cruises Ltd is line with the GDPR, Cyprus SA acquired additional information and namely:

Concerning the collection of health related data prior to employment -
(a) the categories of all health data collected by Sea Chefs Cruises Ltd
(b) anonymized copies of medical records provided by employees

In the event of illness and injury of an employee while serving on board of a vessel-
(c) **the procedure** followed by Sea Chefs Cruises Ltd in relation to the collection and sharing of health related data after the incident (illness and injury)
(d) the categories of all health data collected by Sea Chefs Cruises Ltd
(e)anonymized copies of medical certificates and medical records provided by employees

The company provided in due time all documentation requested, by letter of 12.10.2020.

In their letter the company explained that *"the particular circumstances of the industry sea chefs operates in and the multitude of laws, regulations and agreements we must abide by especially with regards to the crewmembers' health and safety as well as passengers. For this reason, essentially, we cannot employ anyone without collecting and processing their medical data and we are obliged to retain and have available such information. We are also obliged to offer medical care to our crewmembers*." They further pointed out that "*the Authorisation for the release of medical records' clearly states the purposes and reasons such release is requested and very strictly declares that such process will be protected, restricted, limited and only when necessary for the purposes contained therein*."

C. Legal framework

Definition of consent

Article 4(11) GDPR: 'consent' of the data subject means 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.

Article 5: Principles relating to processing of personal data

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 ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Article 7: Conditions for consent

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 9: Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.".

Paragraph 2:

Paragraph 1 shall not apply if –

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject ().

or/ and

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

D. Views of Cyprus SA and Reasoning

As it stands now, the *Authorisation* appears to be based on the consent of the employee. Indeed, under article 9(2)(a) of the GDPR the controller may rely on explicit consent of the data subject for the processing of special categories of data. Cyprus SA underlines that in such a case, various conditions should apply for the validity of the consent: not only should the consent be **explicit** it must also be **freely given, specific and informed** (article 4(11) of the GDPR).

Cyprus SA considers that the condition of freely given consent **does not apply in the present case**, as employees of Sea Chefs Cruises Ltd who are requested to sign the Privacy Notice in advance upon commencement of the employment, have no real choice. They feel compelled to consent and if they do not consent, they will endure negative consequences, and namely they will "*not be offered employment*". Consequently, consent is not considered to be freely given when the employee is unable to refuse or withdraw his or her consent without detriment. In line with article 7(3) of the GDPR, the data subject shall have the right to withdraw his or her consent at any time and the withdrawal of consent **shall not affect the lawfulness of processing based on consent** before its withdrawal.

Moreover, Cyprus SA considers that in the employment sector, in general, consent should not be used as the lawful basis for the processing due to the imbalance of the relationship between employer and employee. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. Reference should be made in this regard to previous decisions of Cyprus SA, [decision against Louis Group Ltd of 12/10/2019, Decision against Gan Direct Insurance of 24/5/2018, Decision against Apollonion Hospital of 02/10/2012] where the authority ordered the controllers to cease the processing, among other reasons, due to the fact that consent cannot be used as the lawful basis for the processing.

In relation to the condition of freely given consent, reference is made to the EDPB Guidelines 05/2020 on consent, which state that:

> The element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or

withdraw his or her consent without detriment. The notion of imbalance between the controller and the data subject is also taken into consideration by the GDPR. (§ 13 page 7)

When assessing whether consent is freely given, one should also take into account the specific situation of tying consent into contracts or the provision of a service as described in Article 7(4). Article 7(4) has been drafted in a non-exhaustive fashion by the words "inter alia", meaning that there may be a range of other situations, which are caught by this provision. In general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid. (§ 14 page 7)

An imbalance of power also occurs in the **employment** context.[1] Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, the EDPB deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.[2] (§ 21 page 9)

It follows from the above that "consent" of the employees provided in the form the "*Authorisation for release of medical records*" of the Privacy notice (issue date 15-03-2019) does not fulfil the requirements of valid consent.

Furthermore, in accordance with the minimisation/ proportionality principle (article 5(1)(c) of the GDPR), the data processed by the controller should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In this regard, Cyprus SA considers that the controller should collect and generally process only data that are absolutely necessary to be able to assist the employees with medical care, to arrange any associated travel and to handle any medical claim, in line with relevant laws and the purposes laid down in Article 12 (Medical Care, Sick Pay and Maintenance) and Article 14 (Death and Disability Compensation) of the Collective Bargaining Agreement.

As previously explained, in the framework of its activities, Sea Chefs Ltd is held to comply with its legal obligations to conform with relevant laws, regulations and international conventions which makes it obligatory for the company to hold and process health-related data of employees, as well as for the purposes set out in the Collective Bargaining Agreement.

According to the explanations given by Sea Chefs Ltd, due to incomplete and/or insufficient relevant medical data provided by employees, the company is constantly exposed to the following risks:

---

[1] See also Article 88 GDPR, where the need for protection of the specific interests of employees is emphasised and a possibility for derogations in Member State law is created. See also Recital 155.

[2] See Opinion 2/2017 on data processing at work, page 6-7.

1. Exposure the crew member and his health to danger, during his repatriation after illness or accident. The responsibility for the safe repatriation of each patient (employee) is assigned to the employer and not to the ship's doctor after disembarkation from the ship. In addition, post-repatriation recovery supervision is still the responsibility of the employer.
2. Failure to properly inform the family of each crew member (next of kin), after illness or accident. Informing the family is a contractual obligation under the Collective Bargaining Agreement .
3. Inability to properly defend a legal case in the event of legal proceedings.
4. Refusal of Maritime Insurance (P&I Club) to pay compensation.
5. Charging the company with the payment of Sickness Compensation for up to 130 days due to failure to submit relevant and sufficient medical data.

Article 9(2) GDPR provides a list of possible exemptions to the ban on processing special categories of data. Apart from consent, Article 9(2) describes nine additional lawful bases on which a controller can rely on.

Cyprus SA was called upon to assess whether the controller could rely on another legal basis for the collection and general processing of employees' health-related data, other than consent.

On the basis of the information available to it, Cyprus SA considers that Sea Chefs Ltd is entitled to process health-related data of employees on the basis of article 9(2)(b) of the GDPR, when the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment in so far as it is authorised by the collective agreement and only where necessary to achieve those purposes for the benefit of employees, in particular in the context of the management of health care services and systems.

Yet, the collective agreement should provide for appropriate safeguards for the fundamental rights and the interests of the data subject. Those safeguards must include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing and the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

On the basis of article 9(2) (h) of the GDPR, Sea Chefs Ltd is entitled to process health-related data of employees, when the processing is necessary for the assessment of the working capacity of the employee, medical diagnosis, the provision of health care or treatment, under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies.

In light of the above, the assessment of the working capacity of the employee, medical diagnosis, the provision of health care or treatment, should only be done under the responsibility of a professional subject to the obligation of professional secrecy and Sea Chefs can only access those data authorised by law and collective agreements.

E. Decision

Cyprus SA assessed all the information available in relation to this case and decided that the consent provided by employees to the controller "Sea Chefs Cruises Ltd", by means of the *"Authorisation for release of medical records*" of the Privacy notice (issue date 15-03-2019), is not in accordance with the rule of Article 4(11) and Article 7 of the General Data Protection Regulation.

Cyprus SA considers that in the employment sector, consent should not be used as the lawful basis for the processing due to the imbalance of the relationship between employer and employee. Sea Chefs Cruises Ltd should explore the specific exceptions in Article 9(2) subparagraphs (b) to (j) to lawfully process health-related data of employees.

In accordance with the minimisation/ proportionality principle (article 5(1)(c) of the GDPR), Cyprus SA considers that the controller should collect and generally process only data that are absolutely necessary to be able to assist the employees with medical care, to arrange any associated travel and to handle any medical claim, in line with relevant laws and the purposes set out in Article 12 (Medical Care, Sick Pay and Maintenance) and Article 14 (Death and Disability Compensation) of the Collective Bargaining Agreement.

In light of the above, and in accordance with the powers conferred to the Commissioner by Article 58(2)(d) of the GDPR, the Commissioner **orders** the controller:

a) to cease the processing of health data of employees based on consent,
b) to bring the processing operations into compliance with the provisions of the GDPR and in particular to take actions as to process only those health related data in the employment context which are necessary for the discharge of obligations laid down by law or by the collective agreements for the purposes of the recruitment, the performance of the contract of employment, health and safety at work, and the exercise and enjoyment of rights and benefits of employees,
c) to inform the Commissioner on the actions taken to comply with this Decision at the latest **within one month** from the date of this decision.

In the event that Sea Chefs Cruises Ltd does not comply with the above order within the aforementioned deadlines, the Commissioner shall envisage additional corrective actions.

The Commissioner
For Personal Data Protection

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA PROTECTION

Our ref. 11.17.001.008.042

17 February 2021

Data Protection Officer
GRS Professional Recruitment Services Ltd
Limassol, Cyprus

Subject: Investigation of complaints concerning a data breach occurred on 11.02.2020

Dear Sir,

Following our exchange of communications concerning the above subject, we hereby inform you on the decision of the Commissioner.

We recall that three complaints were lodged in Malta in February 2020, against the controller GRS Recruitment LTD, and the incident involves two emails sent to 201 recipients on 11/02/2020, providing information about IT job vacancies and in which the email addresses were shown to all recipient (emails were sent with cc instead of bcc). The recipients of the messages were candidates who registered with the controller. The complainants expressed concerns about the possible consequences of the unlawful disclosure of their personal data to third parties.

It is noted that the data breach was notified to the Commissioner by the controller on 12/02/2020 and it was further communicated to the data subjects, in line with articles 33 and 34 GDPR. In the data breach notification submitted on 12/02/2020, you affirmed that the cause of the breach was due to an internal human error and not to a malicious user. Concerning the measures taken before the breach, you stated that the company adheres to the principles of privacy by default, that all employees undertook training on how contacting data subjects, how personal data should be respected and handled, including on how to send job notifications to data subjects. Concerning the actions taken after the incident, you proposed as a corrective measure to impose to employees obtaining the approval of a Director and the DPO of the company before any external email can be sent to more than three data subjects, whilst the employee who made the error, will be subject to a disciplinary hearing and will undertake further training.

In the course of the investigation process of the complaints received, you explained that the procedure of the identification and handling of personal data breaches was effective, since it enabled the controller to notify the breach to the Commissioner within the timeframe foreseen in the GDPR. Moreover, you affirmed that, to date, none of the data subjects instituted legal proceedings against the controller claiming compensation of any damage which the data subject may have suffered as a result of the data breach.

After assessment of all information available in relation to this case, the Commissioner considers that by disclosing the email addresses of candidates to all the recipients, the controller infringed the obligations referred to in Article 32 of the GDPR. The Commissioner further considers that appropriate technical and organisational measures should be taken to ensure the protection of the rights and freedoms of natural persons with regard to the processing of their personal data.

You previously proposed a number of corrective measures to mitigate the risks, however the Commissioner requires additional technical measures to be implemented by the controller to prevent such an incident to occur in the future and namely –

- An alert message to be clearly displayed every time an email is sent to recipients outside the organisations;
- Whenever a mass email is to be sent, an information message shall pop-up on the sender's screen in a manner that cannot be missed and, ideally, preventing the user from proceeding with the sending of the communication unless a positive action is taken, such as, prompting the user to close the message box;
- Disable the cc field or limit the number of email addresses that the field can contain;
- Set up a delay rule in the delivery of any email message.

In light of the above, and in accordance with the powers conferred to the Commissioner by Article 58(2)(d) of the GDPR, the Commissioner orders the controller:

a) to implement the technical measures described above,

b) to inform the Commissioner on the actions taken to comply with this Decision at the latest within one month from the date of this letter

Best regards,

Commissioner
for personal data protection

Our ref. 11.17.001.008.076

[redacted]
Data Protection Officer
Crowd Tech Limited
116 Gladstonos, M. Kyprianou House,
3032, Limassol, Cyprus

Final Decision
Complaint regarding the data subjects request for erasure (IMI 122875)

A complaint was lodged in Germany (SA Schleswig-Holstein) against the controller Crowd Tech's (Trade360.com), a company whose main establishment is in Cyprus. The complaint was transmitted to the Commissioner for Personal Data Protection (Cyprus SA), to be handled as a local case.

We recall that the complaint concerns the controller's failure to comply with the erasure request of Mr. S.P. as well as the absence of consent.

Cyprus SA engaged with the controller on 27/7/2020 and requested information such as
(a) the reasons of not complying with the erasure request of the DS, including the specific legal grounds,
(b) the categories of personal data retained in respect of Mr S.P., and
(c) the source of the data.

Crowd Tech explained that the reason of non-compliance with the erasure request is that the employee who directly received the data subject request, neglected to forward the request to the relevant team and DPO for immediate handling. They further affirmed that Mr. S.P's request has been handled, as soon as the complaint was received and that the DS was informed accordingly on 26/8/2020 that his data was removed. Further to our request, Crowd Tech communicated to us a copy of the email sent to the DS on 26/8/2020 (the document is uploaded in the relevant documents tab).

Crowd Tech further asserts that it received and promptly handled more than four thousand data subject requests since May 2018 and that the relevant DSR registry is available upon request.

As far as the categories of personal data concerning Mr. S.P. Crowd Tech explained that the full name, email address, telephone number and country were collected from the DS and that no further personal and/ or financial information was obtained from Mr. S.P.

As regards to the source of the data, Crowd Tech affirms that the Mr. S.P opened an account with Trade360, and expressed interest in registering. However as per later communications with the employee, it was found that he was not interested in proceeding any further.

In light of the above, Cyprus SA requested from the controller to take remedial actions as to ensure in the future that data subject's rights are recognized **by all employees** and brought to the competent department to handle the request in due course.

Considering the fact that the controller eventually complied with the erasure request, 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.

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.

Best regards,

Commissioner for Personal
Data Protection
Cyprus

REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER FOR PERSONAL DATA PROTECTION

COMMISSIONER

Ref. N.: 11.17.001.009.019

SENT BY EMAIL and BY CERTIFIED MAIL

To: dpo@trade360.com
CC: support@geevosolutions.com; [redacted]

19 October, 2021

Data Protection Officer
Crowd Tech Limited
P.O. Box 53244
3301 Limassol

Dear Sir,

FINAL 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

A complaint was lodged in Poland against the controller Crowd Tech's (Trade360.com), a company whose main establishment is in Cyprus. The complaint was transmitted to the Commissioner for Personal Data Protection (Cyprus SA), to be handled as a local case.

We recall that the complaint concerns the controller's failure to comply with the erasure request of Mr. [redacted] and the withdrawal of the data subject's consent on 25.11.2020.

Investigation by CY SA

Cyprus SA contacted with the controller on 11.2.2021 and requested various information, and more particularly for this complaint:

1. The source of the data of the complainant.
2. The legal basis of processing for the calls made to the complainant.
3. If the processing was based on consent, specific evidence.
4. The reason why the erasure request of the complainant was not complied by the controller.

Crowd Tech explained the following:

1. The source of the data of the complainant was him, when he registered over landing page on 20.7.2020 09:20 from the IP address [redacted] (specific evidence provided such as screenshots of the registration information stored into their systems).
2. The legal basis of processing was consent. The data subject entered the information and submitted it over a click of a button in order to be further contacted, during the registration process.
3. Specific landing page with the link of the process, provided.
4. The reason of non-compliance with the erasure request is that the complainant's claimed request for data erasure was never clearly stated or provided in writing. It was just mentioned over the said calls without clearly clarifying the initial request, while at the same time the caller (Service Provider of Crowd Tech) informed the complainant that the initial request could not be found into their systems. Furthermore, the complainant never gave the opportunity to the Service Provider to service and assist. Instead there was cut off in phone conversations.

The complainant on 13.7.2021, provided CY SA with an unofficial translation (throughout the Poland Authority and the IMI system) of the conversation he had on the 25.11.2020 at 13:58, with the caller, an employee of the Controller's Service Provider (i.e. the Processor). Within the conversation, the complainant withdraws any consent given, saying that he does not want to be called anymore and would like his data to be erased (Art. 6(1)(a) and Art. 17(1)(b) of the GDPR). He specifically said: *"But the last time we talked, I asked you to erase my data from your database. I would like to exercise the right to be forgotten. That was about to be done and nobody should not be calling me anymore"*. The Processor's employee replied that she did not have this kind of information into their systems. The complainant responded that he has recorded the specific conversation and will proceed and send it to the right place, thanking the Processor's employee and saying that he will talk to her later. Then the Processor's employee replies, "Talk to you later".

According to the content of the complaint, the complainant received another two calls. One on the same day (25.11.2020 at 14:24 from another person belonging to the Processor's team) and one the next day (26.11.2020 at 12:37 from a third person belonging to the Processor's team). The Polish Authority did not provide us with the content of those two conversations, even though they seem to be attached in mp3 format on the original complaint. Within the written complaint sent, the complainant also expressed the following:
"...despite the notification company Trade360 ... about my request to realize my right to be forgotten still I revive harassing phone calls from persons claiming to be employees of Trade360 and inciting me to invest in the FOREX platform. I have records of three last conversation with them (attachments). In each situation I informed that earlier I demand my right to erasure my personal data."

In a complementary letter of the complainant to the Polish Authority on 14.12.2020, the complainant says:
"... I am not able to say whether the obtained data comes from me or was obtained in a different way than from me, therefore I am not able to determine which article of the

GDPR is appropriate here. I was not informed during telephone calls where my data came from".

Within the transcript we have been provided on 13.7.2021 the Processor's employee says to the complainant:
"... I'm calling to you from the firm Trade360... lately we have been talking about the investing through the trading platform. Could you please tell me, if you can talk right now?". The complainant did not refuse that they have talked through the trading platform. What the complainant said after that, is that the last time they have talked, he asked his data to be deleted from the database.

Throughout the investigation of the complaint, the Controller clarified to us that the complainant was registered as a client on 20.07.2020 from the IP address [redacted] through a landing page with the following link: [redacted] Screenshot was attached. Actual identification of a person registering an account takes place in a Know-Your-Client (KYC) process and by that any successful process becomes an activated account and therefore prospective client turns into an actual client. As regards physical person consent, any data subject can freely register over a landing page and submit registration details by a click of a button, therefore a clear affirmative action to be further contacted. The Controller use submitted data to contact registered persons. The Controller's position was that the complainants claimed request for data erasure was never clearly stated or provided in writing. In the contrary, it was just mentioned over the said calls without clearly clarifying the initial request, while at the same time the Processor's employees were informing the complainant that no such request could be found into their systems. The complainant never gave the opportunity to the Processor's agents to service and assist. The complainant has been requested to give more information in order to track his deletion request, he never replied, and the call was disconnected.

The Controller provided an excel file to our office, containing all the data subject's requests, the way those were submitted, and the department handling the requests. All the requests were submitted either through email or though the chat platform. Almost all the requests were handled by the Customer Support department and some from their Compliance Department/DPO.

The Controller affirmed that the complainant's request has been handled, as soon as the complaint was received by our Authority on 11.2.2021. Within the excel file provided it is stated that the complainant's request for data erasure was fulfilled on 11.2.2021 by their Compliance Department/DPO.

At this stage, it should be said that both the Controller and the Processor are companies authorized and regulated by the Cyprus Securities and Exchange Commission. Under art.17(7)(6) and 17(7)(h) of the national Law 87(I)/2017, an investment company is obliged to keep records of all services and activities provided, and transactions undertaken by it, which shall be sufficient to enable the Commission to exercise its supervisory functions for a period of five years and, where requested by the Commission, for a period of up to seven years. There are also other regulatory obligations (for example anti money laundering "AML") which might prevent a company from completely deleting a data subject's data (please see Art. 17(3)(b) of

GDPR). However, an investment company can fulfil a data subject's request, not to be further contacted by phone.

Although we do not know the content of the other two conversations made between the complainant and the Processor's employee, we believe that the Processor should have assisted the complainant to his request, even though this was not made in writing. The complainant clearly expressed his wish not to be further contacted and clearly claimed his right to be forgotten. Therefore, the complainant's request for deletion was successfully lodge on 25.11.2020. The Processor did not act on behalf of the Controller, despite the fact that within their Service Agreement the Processor warrants that "it will immediately inform the Company if in its opinion an instruction infringes the law and/or any data protection regulations" or the fact that within the same Service Agreement, the Controller undertakes full responsibility "to its customers for any action or omission on the part of the Contractor" (i.e. the Processor).

Therefore, when the complainant expressed his oral request, the Service Provider and consequently the Controller, had a duty under Art. 12(2) and Art. 24 to facilitate the exercise of his rights by implementing the appropriate technical and organisational measures to handle such oral requests. The oral request owed not to be neglected and the data subject should be assisted with the fulfilment of his request. The Processor's employee was either not properly trained or the Controller's directions to the Processor regarding the data subject's requests, were not clearly stated.

Consequently, when the complainant's data was finally deleted on 11.2.2021, the Controller did not comply with the deadline established in Art. 12(3) of the GDPR for response within one month from receipt of the request. Additionally, when the complainant withdrew his consent on 25.11.2020, the Controller did not have any other legal basis for the processing after the erasure request. Therefore, the Controller processed complainant's personal data unlawfully, according to Art.6(1)(a) of the GDPR, and did not take any measures regarding the complainant's request when the personal data were no longer necessary in relation to the purposes for which they were collected (i.e. to contacting registered persons) (Art. 17(1)(b)). Finally, the Controller had a duty under Art. 24 of the GDPR, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation.

Commissioner's view and corrective actions

Having in mind all the above, as well as the fact that the Controller, within the Service Agreement, is deemed fully and unconditionally liable towards its clients, for any action or omission taken on the part of the Processor when providing services to the Controller, I find the Controller liable for violations of the Articles 6(1)(a), 12(2), 12(3), 17(1)(b) and 24 of the GDPR.

Under the powers vested to the Commissioner for Personal Data and having in mind all the facts of this case, the Commissioner **issues a reprimand to the Controller - Crowd Tech Limited,** pursuant to Art. 58(2)(b). For this conclusion, the Commissioner takes into consideration the fact that the data subject's request was finally fulfilled. It also takes into consideration the cooperation of the Controller, throughout the whole process of the investigation.

The Commissioner additionally **orders the Controller - Crowd Tech Limited,** to implement appropriate technical and organisational measures so as to ensure that all the data subject's requests are recognized and handled appropriately by its staff. The Controller shall inform the Commissioner, within a period of 3 months after receiving this decision, regarding the measures taken for the fulfilment of the above order.

[redacted]

Commissioner
for Personal Data Protection

Final Decision

Case Register	296225
National file number	11.17.001.009.085
Controller	GG Influencing Central Ltd
Date	15.12.2021

[redacted]

GG Influencing Ltd
Arch Makariou III, 59
6017 Larnaca, Cyprus

Dear Sir,

Further to the exchange of communications between Cyprus SA (the Commissioner for Personal Data Protection) and GG Influencing Central Ltd (the Controller) concerning a complaint involving an erasure request, we would like to bring to your attention the following assessment of the Commissioner.

Description of the Case

The data subject (DS) lodged a complaint with the Romanian SA, and was thereafter received by the Office of the Commissioner for Personal Data Protection (Cyprus SA) on 21 January 2021. The complaint involved the Controller's failure to comply with the DS erasure request (article 17 of the GDPR) submitted to the Controller, who operates the website www.gg-influencing.com.

The DS, who is a former client of the Controller, submitted his erasure request via email to contact@gg-influencing.com on 5 April 2020, where he specifically withdrew any consent and demanded that his personal data was erased as per article 17 of the GDPR. After not receiving a reply, the DS lodged a complaint regarding the Controller's failure to fulfill the request since the videos concerning him were still posted on the controller's YouTube and Instagram channel.

Investigation by Cyprus SA

The Commissioner's office contacted the Controller using the email address mentioned in their website, and requested their views on the matter raised by the complainant. Upon not receiving a reply, the email was forwarded again to a different email that belonged to the controller, which was obtained through a partner company of the Controller.

The Controller's Director replied the same day and informed the Commissioner's office that, due to the inactivity of the email address contact@gg-influencing.com, the email sent to this address by the Commissioner's office was never received. Nevertheless, he stated that he had already complied with the complainant erasure request since he had removed all detected related videos from the relevant YouTube channel. He also added that he removed the complainant's email subscription and all his details from the internal system.

In the Commissioner's office response, the Director was informed that according to the information provided by the complainant, as also a further investigation, it appeared that the complainant's personal data was still being processed through YouTube and Instagram accounts that the controller is administrating. He was also requested to proceed with:

I. the erasure of the complainant's personal data as seen in the relevant links provided.
II. the update of the contact information provided on the website so that the controller is able to respond to the inquiries of the data subjects and the Commissioner's office which is the National Supervisory Authority as per the GDPR, as is the obligation as data controller.

The Controller responded on the same day and complied with the above requests.

Cyprus SA assessment

Considering the fact that the Controller eventually complied with the erasure request, 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.

After consideration of the significance of the infringement and the controller's cooperation in the investigation process, the Commissioner considers that the investigation proceedings to be concluded as no further supervisory measure is necessary at this stage.

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

REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Our ref.: **11.17.001.008.217**

3 January 2022

Decision

Failure to Fully Comply to a Subject Access Request by Playkot Ltd

A complaint was lodged in Germany (Hessian Commissioner for Data Protection and Freedom of Information) against the company Playkot Ltd (the controller), whose main establishment is in Cyprus and the complaint was subsequently transmitted to the Commissioner on 07.07.2020, 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.

Case Description

3. The controller, Playkot Ltd, is a company that develops games and offers web services and other related services. [redacted], the complainant, who uses the services provided by the controller, claimed that he contacted the controller several times requesting access to information for all processing done on his personal data as per Article 15 of the General Data Protection Regulation (GDPR). He also stated in his complaint that, he was only provided with a link to the privacy policy of Playkot Ltd and no other information regarding his request.

4. My Office engaged with the controller via email on 9 December 2020 and following the exchange of several communications in relation to the subject matter of the complaint, the following information was provided by the controller's legal representative on their email dated 8 January 2021:

i. The complainant sent an initial Subject Access Request (SAR) via email on 26 January 2020. The complainant requested to be informed of all his personal data that are processed by the controller. Specifically, he requested full details about data stored about him and his account, the relevant processing and the type and scope of the data transfer to third parties including any processing done in the context of Google Play Store. He repeated his request through the controller's in-game support system on 7 February 2020.

ii. On 8 February 2020, a representative of the controller responded to the email and requested for him to specify what information was needed by the complainant. The representative did not receive a reply, and thus the relevant support ticket was closed automatically on 12 February 2020.

iii. On 11 March 2020, the complainant sent a follow up email reminding the controller that his request was not satisfied, to which the controller did not reply.

iv. On 2 April 2020, the complainant sent a second Subject Access Request and requested any information regarding his personal data. Specifically, he asked *"...for information in accordance with Art. 15 GDPR. Please confirm whether you are processing personal data concerning me (Art. 4 No. 1 and 2 of GDPR).*

In this case, I ask you in accordance with Art. 15 Paragraph 1 of GDPR for information about all personal data that you have stored about me; the purposes of the processing; the categories of personal data that are processed; the recipients or categories of recipients to whom the personal data have been disclosed or are still being disclosed; if possible, the planned duration for which the personal data will be stored or, if this is not possible, the criteria for determining this duration; if the personal data were not collected from me, all available information about the origin of the data; If applicable, the existence of automated decision-making including profiling in accordance with Art. 22 Paragraph 1 and 4 of GDPR and - if given - meaningful information about the logic involved and the scope and intended effects of such processing for my person.

If you transfer my personal data to a third country or to an international organization, please be informed about the appropriate guarantees in accordance with Art. 46 of GDPR in connection with the transfer."

v. A representative replied to the above request on the same day by providing a link to the controller's Privacy Policy.

vi. The complainant also made other game related requests during the same period via the same in-game support system.

vii. On 28 December 2020 and on 8 January 2021, a support team supervisor of the controller contacted the complainant via the support system and provided him with additional information regarding the processing of his personal data.

5. On 5 February 2021, the controller's legal representative, sent an email informing my Office, that the complainant replied on 9 January 2021 acknowledging the reception of the information provided on 28 December 2020 and on 8 January 2021, but requested that they also sent him all his personal data stored by the controller. The complainant's last request was eventually satisfied on 21 January 2021 through a corresponding reply from the supervisor.

6. On 31 March 2021, the controller updated my Office via telephone and email, that the complainant informed them that his request was fully satisfied and he withdrew his complaint towards the Hessian Commissioner on 15 March 2021.

Preliminary Decision

7. On 12 October 2021, the Commissioner issued a Preliminary Decision, taking into consideration that:

i. The initial SAR on 26 January 2020 was not satisfied at all and
ii. The information provided in response to the second SAR on 2 April 2020 was not satisfactory and in line with the information as per Article 15 of the GDPR

Moreover, it was determined that the controller had not complied with the complainant's request in a timely manner, ensuing a violation of Article 12(3) of the GDPR.

8. The controller's legal representative responded on 16 November 2021, to the Preliminary Decision and stated, inter alia, that:

i. The controller accepts that the initial SAR was not given the appropriate attention in order to satisfy the complainant's request. It is also understood that sending the privacy policy as a response to the second SAR is not considered satisfactory as per Article 12(3) GDPR.
ii. The controller did not receive a reminder to the second SAR, and therefore it was incorrectly concluded that the request was satisfied by the information provided on the privacy policy. Despite this, it is emphasized that the controller did not act in bad faith.
iii. As soon as the controller was made aware of the complaint by my Office, the complainant was contacted again so as to resolve the issue as effectively as possible.
iv. Following the above communication, the complainant withdrew his complaint to the Hessian Commissioner.

9. In addition to the above, the controller's legal representative included the following mitigating factors to be taken into account, inter alia, by the Commissioner:

i. The controller did not act in bad faith and all the omissions took place due to lack of experience on GDPR related matters.
ii. The controller did not benefit or take any advantage of the complainant's rights or data as a result of the possible violation mentioned in the Commissioner's Preliminary Decision.
iii. The systems and procedures in place related to GDPR related communications and satisfaction of data subject requests have been improved following the complaint.
iv. The support team has been educated on handling GDPR requests and the Information Security Framework has been improved.
v. The specific complaint was a remote incident to the best of the controller's knowledge.

Legal Framework

10. 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.*

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.

Views of the Commissioner

12. 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 correct procedures on GDPR related matters as also a lack of appropriate attention to the complainant's request, I consider that the controller comprehends 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.

13. Despite this, considering that the GDPR had been enforced for almost 2 years 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.

14. Furthermore, as regards the second SAR, the privacy policy cannot in any case constitute information pursuant to Article 15 GDPR to a data subject since, no **specific** information was provided regarding the processing of the complainant's personal data. Article 13 GDPR requires completely different information than Article 15 GDPR, in particular than Article 15(3) GDPR.

Decision

15. 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 Playkot Ltd of Article 12(3) of the GDPR, since the controller has not complied with the complainant's request in a timely manner.

16. 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 (4-5) factors:

1. That there is no previous violation by the controller of the GDPR 2016/679.
2. The willing cooperation and the responses to our inquiries without delay.
3. The withdrawal of the complaint.
4. None of the two SARs were satisfied in a timely manner.
5. The lack of appropriate procedures and measures for handling data subject rights.

17. 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 Playkot LTD for the infringement mentioned in paragraph 16 above. In the event of a recurrence of a similar infringement within 12 months from today, this Decision may be counted against the company.

Final Decision

Case Register	329048
National file number	11.17.001.009.220
Controller	At Bookshouse Ltd
Date	07.01.2022

[redacted]
[redacted]
[redacted]At Bookshouse Ltd
[redacted]

Dear Sir,

Further to the exchange of communications between Cyprus SA (the Commissioner for Personal Data Protection) and At Bookshouse Ltd (the Controller) concerning a complaint involving an erasure request, we would like to bring to your attention the following assessment of the Commissioner.

Description of the Case

[redacted] the data subject lodged a complaint with the German SA Rhineland-Palatinate, and was thereafter received by the Office of the Commissioner for Personal Data Protection (Cyprus SA) on 13 April 2021. The complaint involved the Controller's failure to comply with the data subject's erasure request (article 17 of the GDPR) submitted to the Controller, who operates, amongst others, the website www.bookshouse.de.

The data subject, [redacted], stated in her complaint, that she contacted the publisher (the Controller), requesting, among other things, the termination of her contract and the deletion of her personal data from the publisher's records and from its websites (www.bookshouse.de and others). The data subject mentioned that she sent a letter by registered post/mail on 10/02/2021 that was delivered on 04/03/2021 and she additionally sent an email on 11/02/2021 addressed to all email addresses of the Controller. She claimed that she did not receive an answer to her erasure request and that her data and work were still advertised and viewable on the publisher's website.

Investigation by Cyprus SA

The Commissioner's office contacted the Controller via its [redacted] and requested, through email, their views on the matter raised by the complainant.

The Controller's [redacted] replied to the Commissioner's office, and among others, provided the following information:

the Controller has deleted the data subject's data

the Controller ceased its operations and has started the procedures to liquidate

the Controller has closed all its websites and currently does not have any active websites.

Cyprus SA assessment

Taking into account the fact that the Controller eventually complied with the erasure request, 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.

After consideration of the significance of the infringement and the Controller's cooperation in the investigation process, the Commissioner considers the investigation proceedings to be concluded as no further supervisory measure is necessary at this stage.

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

Final Decision

Case Register	379610
National file number	11.17.001.009.186
Controller	Trustona Media Limited
Date	2/9/2022

Trustona Media Limited
By email: info@trustonamedia.com

Dear Sir,

Further to the exchange of communications between Cyprus SA (the Commissioner for Personal Data Protection) and Trustona Media Limited (the Controller) concerning a complaint involving the use of tracking cookies on the Controller's website.

Description of the Case

The data subject (DS) lodged a complaint in Germany with the North Rhine-Westphalia SA, and was thereafter received by the Cyprus SA on 13 July 2021. The complaint involves the use of tracking cookies without consent through the Controller's website, www.coffeeness.de.

[redacted] (the complainant) stated that while visiting the website www.coffeeness.de he noticed that certain tracking cookies were enabled during the browsing session without giving his explicit consent. Following this, on 3rd of May 2021 he sent an email to info@coffeeness.de requesting that these cookies must be removed, to which he did not receive a reply. After not receiving the requested information, the data subject lodged a complaint on 1 June 2021, regarding the controller's failure to remove the tracking cookies.

The complainant also provided relevant documentation which demonstrated that the cookies which were enabled during his browsing session were Facebook Pixel and Google Analytics.

It is also noted that the complaint involves the use of cookies which falls under the ePrivacy Directive and thus it cannot be handled in accordance with the procedure provided in Article 60 GDPR. Despite this, considering that the cookies were already set prior to the complainant's consent, the Cyprus SA has investigated the legal basis for the possible collection and processing of the complainant's personal data under the GDPR.

Investigation by Cyprus SA

Cyprus SA carried out an examination of the website and it was determined, among other things, that pre-activated tracking cookies were found in addition to the necessary cookies before any consent was given. The cookies that are activated on the website before receiving consent of the visitor which do not fall into the category "Necessary Cookies" were the following:

Mautic_device_id (tracking)
mtc_id (marketing)
mtc_id (tracking)

Although the Google Analytics and Facebook Pixel cookies were detected on the website, they were not enabled before any consent was given.

Moreover, as per the Cyprus SA request, the Controller proceeded without delay with the appropriate changes on the website to comply with the ePrivacy Directive and the GDPR.

Cyprus SA assessment

Considering the fact that

i. Although the Controller did not respond to the complainant's email on 3/5/2021, they had indeed configured, at a later stage, the Google Analytics and Facebook Pixel cookies to be enabled only upon receiving consent from the website visitors.
ii. the tracking cookies that were enabled without consent at the date of the Cyprus SA examination, were removed by the Controller as soon as they were notified

Cyprus SA is of the view that the above observations appear to be a minor infringement which only slightly affects data subject's rights and freedoms.

After consideration of the significance of the infringement and the controller's cooperation in the investigation process, the Cyprus SA considers that the investigation proceedings can be concluded as no further supervisory measure is necessary at this stage.

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

Final Decision

Case Register	347222
National file number	11.17.001.009.245
Controller	F1Markets Ltd
Date	2.9.2022

2 September 2022

F1Markets Limited
gdpr@f1markets.com
gdpr@investous.com

Dear Sirs,

Further to the exchange of communications between Cyprus SA (the Commissioner for Personal Data Protection) and F1Markets Ltd (the Controller) concerning a complaint involving the controller's failure to fulfil the complainant's erasure request, please note the below:

Description of the Case

The complainant lodged a complaint with the North Rhine-Westphalia SA in Germany, and was thereafter received by the Office of the Commissioner for Personal Data Protection (Cyprus SA) on 3 May 2021. The complaint involves the controller's failure to comply with the DS erasure request (SAR) (article 17 of the GDPR) submitted to F1Markets Ltd (the controller), which operates the website www.investous.com.

The complainant states that, he requested from the company through email, to permanently delete his personal data and although he was informed by them (through email) that his account was closed and that his request for deleting his personal data (including his contact details) was dealt with, he continues to receive unwanted advertising/promotional calls, several times a day.

The complainant also claims that the calls he receives are from different call centers and when he inquired some of the callers, they mentioned his trading account with investous.com. Furthermore, he believes that his personal data (such as telephone numbers, email and postal address) have been shared by Investous/F1Markets to third parties without his consent. When he confronted the controller with this, he was informed by email dated 08.01.2021 that his account had been closed and his request regarding the deletion of personal data had been dealt with, so they no longer had any contact details. However, the complainant did not find this credible because he receives "up to 8 calls a day from different call centers, all referring to his account with Investous when asked".

Investigation by Cyprus SA

The Cyprus SA engaged with the controller and following the responses of the DPO in relation to the subject matter of the complaint, the following information was gathered.

When the DPO of the controller received the complainant's request for data erasure, he was informed on 22 June 2020 (see relevant documents), that as it was stated in the website's privacy policy, they are unable to delete his data before the expiration of the timeframe provided by the relevant laws, as they are required to retain such information for compliance with legal obligations under applicable EU laws and regulatory requirements in line with Article 17 (3) (b) and (e) GDPR.

He was also assured that his personal data would not be used for any other purpose (including product-related purposes, marketing or promotional purposes) nor shared with any other company and they would no longer contact him, unless he requests it or they are legally obliged to do so.

In order to demonstrate their compliance with the above, the controller shared with the Cyprus SA screenshots (see relevant documents) that validated the following:

i. The client was moved to a 'GDPR pool' in the Customer Relationship Management software (CRM) in order to be visible only to those employees who need to have access to the client's account for compliance reasons
ii. The Client's telephone number was archived and replaced with '999999'
iii. All marketing means were blocked
iv. A *'must read note*' was added in the related account in German (account's language), that informs all employees about client's request not to be contacted again *'BITTE NICHT WIEDER DEN KUNDE KONTAKTIEREN- GDPR ANGEFORDER'*

The controller also mentioned that it is a mandatory step to read and acknowledge the Company's privacy policy prior to opening an account with F1Markets Ltd, which was verified by the Cyprus SA.

Additionally, the controller stated that it is against their best interests to share clients' data with third parties or other competitors that intend to trick their clients into engaging them to file complaints against the Company.

Cyprus SA assessment

Considering that,

i. The controller was able to demonstrate credibly that they fulfilled their obligation to respond to the DS erasure request.

ii. The controller took all necessary steps to ensure that the complainant would not be contacted again in any way for marketing purposes.

iii. There is no indication, besides the complainant’s claims, that the controller shared/leaked the complainant’s personal data to third parties.

iv. There is also a possibility that the complainant may have had his data harvested by malicious third parties with the intention of defrauding him.

Cyprus SA has decided to dismiss the complaint and has concluded the investigation involving F1Markets Ltd.

Commissioner
for Personal Data Protection
Cyprus

REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER FOR PERSONAL DATA PROTECTION

Ref: 11.17.001.008.104

28 April 2023

Decision

Complaint against *The Drivers Rent a Car LTD*

[redacted] (the complainant) has lodged a complaint with the Poland SA against *the Drivers Rent a Car LTD* (the Controller) that was received on 10/7/2020 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 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.

Summary of the Complaint:

3. The complainant has rented a car from the Controller. During the rental registration process, he was asked to provide his full name, residence address, phone number, hotel name address and room number, data from his national ID card, PESEL number, driver's license with the issue date, and passport number and series.

4. The complainant claims that he was not informed about the processing of his personal data pursuant to Article 13 of the GDPR. He also mentions Article 15(3) but he does not specify whether he has submitted a request in this regard.

5. Furthermore, he claims that once he was in the car, he discovered that the car was equipped with a monitoring camera and possibly a GPS tracking system.

1, Iasonos Street, 2nd Floor, 1082 NICOSIA / P.O.Box 23378, 1682 NICOSIA – CYPRUS, Tel. +357 22818456, Fax +357 22304565
E-mail: commissioner@dataprotection.gov.cy, Website: http://www.dataprotection.gov.cy

Legal Framework

6.1. 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.

6.2. 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.

Investigation by Cyprus SA

7. After investigating the complaint it was found that the company does not have cameras or GPS devices installed in their cars. In the event that in the future certain cars have a GPS facility, they will be informing the customer in writing. The specific car that the complainant has rented was imported from Japan and the device that is installed in the specific car, is a device used in Japan for automatic toll payment ("ETC" box wired into cars in Japan). The device is inactive / not functioning.

8. As regards the information provided to the data subjects, the controller has informed the Commissioner the following, for fulfilment of the complainant's request for information based on Article 13:

- The identity of the controller is listed on the form that the complainant has signed (and has attached with his complaint)
- The purposes of the processing are:
    - contract purposes.
    - accounting and tax purposes,
    - insurance purposes, (stated on the contract signed)
    - Police purposes (e.g. in cases where offences are performed with the use of the rented car)

  on the basis of processing for the compliance with legal obligations, the performance of a contract, and the legitimate interests pursued by the controller (e.g. safety of his property)
- The recipients of the data are the following:
    - External Accountant for accounting purposes
    - Legal Advisor(s) only in cases of legal actions
    - Insurance company
- The retention period of the rental contract is 7 years as mandated by the tax legislation (for purposes of inspection from the tax authority)
- The data are not transferred to third countries
- There is no automated decision making or profiling,

- The data are not further processed for other purposes.

The Controller does not have a certificate in accordance with Article 43 of the GDPR.

Assessment

9. Based on the above, the controller has infringed Article 13 for not providing the necessary information to the complainant at the time of the collection of his data.

10. Based on Article 58(2)(b) the Commissioner issues a **reprimand** to the Controller for the above infringement.

Right of an effective remedy

11. 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.

Irene Loizidou Nicolaidou
Commissioner for Personal
Data Protection
Cyprus

REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Our ref.: **11.17.001.009.232**

7 September 2023

Decision

Failure to Fully Comply to an Erasure Request by Freedom Finance Europe Ltd

1. A complaint was lodged with the Federal Commissioner for Data Protection and Freedom of Information in Germany (Berlin SA) against Freedom Finance Europe 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 18/9/2021, 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 involved the Controller's failure to comply with the complainant's erasure request (article 17 of the GDPR) submitted to Freedom Finance Germany TT GmbH in Germany which is a subsidiary of the Controller.

3.2. In her complaint, the complainant stated that she initiated a registration process, through the Controller's webpage (https://freedomfinance.eu/), but did not complete the verification required. Following this, she sent an email on 26/01/2021 at clients@freedom24.com requesting the deletion of her data.

3.3. On 10/02/2021 she sent a reminder to the same email address and on 15/2/2021 she got a reply from an investment consultant of Freedom Finance Germany TT GmbH, informing her that the verification process was not completed and asking her whether she needed any assistance. She replied back the same day, requesting again the deletion of her data, together with a corresponding email confirmation. As she claims, she never got a reply.

3.4. Upon receiving the complaint, the Berlin SA requested the views of the subsidiary in Germany on 22/6/2021. The Berlin SA received a reply by the subsidiary on 22/07/2021, through which they were informed, the following:

a) the complainant's emails were lost, and therefore not answered, due to the abundance of communication via email address clients@freedom24.com,

b) the complainant's personal data that were processed were her name and email address,
c) the data were processed for the purpose of opening a demo account, and by opening a demo account, the data subject agreed to the Controller's General Terms and Conditions and consequently to the data processing,
d) the complainant's data was deleted immediately upon receipt of the Berlin SA's letter.
e) the complainant's erasure request was not sent to the appropriate email address. More specifically, the email address clients@freedom24.com, is used for initial customer communication, to which the DPO does not have access. Additionally, data protection enquiries should be sent to email address info@ffineu.eu or to the DPO's direct email address dpo@ffineu.eu, as it is clearly stated in the Privacy Policy.

Investigation by Cyprus SA

4.1. The Commissioner's Office contacted the Controller on 19/4/2022, and requested their views on the matter raised by the complainant as also proof that the complainant's personal data had been deleted.

4.2. In their reply, the Controller confirmed that the complainant's personal data was deleted on 25/6/2021 and provided proof in the form of a screenshot from the relevant database, which was deemed satisfactory. The Controller also provided the relevant email communication where the complainant was informed of the erasure. It is noted that the email was dated 25/4/2022, i.e. after the reception of the email from the Commissioner's Office.

4.3. The privacy policy, which can be found on the Controller's website, clearly states the appropriate email to be used for data protection matters. Despite this, the complainant sent her requests to an email that is used for initial customer communication and receives a large number of emails daily.

Preliminary Decision

5. On 31 May 2023, the Commissioner issued a Preliminary Decision regarding the controller's failure to notify the complainant of the erasure of his data. In the said Preliminary Decision, the Commissioner concluded that

a. Although it is evident that the controller did not have any intention of not satisfying the complainant's request, the controller did not notify the complainant of the erasure of his data within the timeframe set in Article 12(3) GDPR.
b. The Controller should have implemented appropriate technical and organizational measures to ensure that all emails received by employees relating to data subject rights are acknowledged without further delay in accordance with Article 24(1) GDPR.

6. The controller's legal representative responded on 26 June 2023 to the Preliminary Decision and stated, inter alia, that:

a. The personal data concerned, only included the name and email address of the complainant and was not submitted to further processing other than the initial registration.
b. Instead of sending his request to the email addresses mentioned in the privacy policy, the complainant used the German subsidiary's email address clients@freedom24.com along with the personal email of one of the employees of the German subsidiary.
c. With the deletion of said data the complainant did not have access to his profile thus it can reasonably be assumed that the controller provided the complainant with a clear message that the data was deleted.
d. The inadvertent mistake of the employees of the German subsidiary is found in not forwarding the deletion request to the relevant employees in time.

7. In addition to the above, the controller's legal representative included the following mitigating factors to be taken into account by the Commissioner:

a. the nature, gravity and duration of the breach, taking into account the nature, extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage suffered by them.
b. The absence of any element that implies bad intentions from the controller towards the complainant.
c. The absence of any precedent at the expense of the controller.
d. The absence of any benefit ultimately derived by the controller from the alleged infringement.
e. The immediate compliance with the complainant's request once received from a non-generic corporate e-mail.
f. the non-notification of the action to the complainant was an isolated event that, in the light of the company's experience, the procedure has now been modified as the Commissioner states in her letter to prevent it from happening again.
g. the full cooperation with the competent Control Authority to remedy the violation and limit its possible adverse effects.
h. the intention compliance by immediately improving the company's regulations in order to prevent a recurrence of the incident.

Legal framework

8.1. 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.

8.2. Article 17: Right to erasure ('right to be forgotten')

"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).
..."

8.3. Pursuant to article 24(1) of the GDPR *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, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

8.4. 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;
...(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;

Views of the Commissioner

9. Firstly, following the controller's claim in paragraph 6(c), I consider that it cannot be assumed that the inability of the complainant to sign in to this account, is considered as a notification that his erasure request was satisfied. Furthermore, the information provided following Article 12(3) GDPR should be transmitted in a clear and concise manner.

10. 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. I also consider that the controller did not intend to act in a way that would negatively affect the complainant's rights and freedoms.

11. Despite this, considering that the GDPR had been enforced for more than 2 years at the time of the complainant's first erasure request, 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 been informed of the satisfaction of his request without delay.

Decision

12. 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 Freedom Finance Europe Ltd of Article 12(3) and 24(1) of the GDPR, for the reasons mentioned above.

13. Moreover, following an infringement of Article 12(3) and 24(1) 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.
2. The controller satisfied the erasure request as soon as the mistake was realised.
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 erasure request after being notified of the complaint by my the Berlin SA.
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.

14. 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 Freedom Finance Europe Ltd for the infringement mentioned in paragraph 12 above. In the event of a recurrence of a similar infringement within 12 months from today, this Decision may be counted against the company.

[redacted]

Commissioner
For Personal Data Protection

REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Our ref.: **11.17.001.010.007**

4 October 2023

Decision

Requesting Excessive Identification Information to Comply to a Subject Access Request by Technius Ltd

A complaint was lodged with the Netherlands DPA against Technius 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 23/12/2021, 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 countries were identified as being concerned by this case.

Description of the case

3. The complaint was filed against Technius Ltd which manages the website stripchat.com that sells live access to nude models. The complaint included the following information:

3.1. The complainant was informed through online media that the website StripChat had suffered a data breach. Following this, he searched his mailbox and discovered that on 22/10/2019, someone other than himself, registered/created an account at StripChat using his personal email account. He then contacted the controller through the support email address help@stripchat.com on 17/11/2021, requesting to receive a copy of his personal data held by the company, following the provisions of Article 15 GDPR. Additionally, he enquired whether his personal data was affected by the above data breach.

3.2. On 01/12/2021, the controller replied via email address legal@stripchat.com, informing him that in order to proceed with his request, he had to submit a government issued identification document, to verify the identity of the person requesting the data. In his reply, the complainant insisted that requesting a government ID would be excessive since he has made a request using his email address and thus no further identification would be required.

3.3. The complainant was further informed that the data which was processed by the controller and was related to his email address, was the IP address and username that was collected during the account registration. The controller also mentioned that if the complainant wanted to receive a copy of these data, they

need to identify him, or alternatively, they could remove the said data completely from their system.

3.4. The complainant replied and stated that someone else had created the account on StripChat using his email and also that he was not notified of the data breach He also refused to provide any copy of identification document. The controller in their response, informed the complainant that the account would be deleted as it was created fraudulently and also referred him to the notification of the data breach on the website's blog post.

3.5. The controller also informed him that due to the nature of the incident, they were not in a position to identify the exact data that was affected by the breach. The complainant responded that he could confirm that his personal data was affected by the breach through an alert he got by the SpyCloud service.

4. In summary, on the basis of the allegations of the complainant, the controller:

i. only made a public announcement through a blog post, instead of personally informing him through email, and through the blog announcement he could not determine whether his personal data was affected by the incident,
ii. has processed incorrect personal data and stored it for more than two years,
iii. requested him to submit an identification document in order to fulfill his access request.

Investigation by Cyprus SA

5.1. The Commissioner's Office contacted the Controller on 11/2/2022, and requested their views on the matters raised by the complainant and, among others:

i. The reason for not informing each data subject individually about the breach.
ii. The legal basis under which an identification document is required to respond to a data subject's access request, or any other right (e.g., right to erasure, to rectification, etc.).
iii. The reason for not satisfying the data subject's request by providing the information directly to the connected email.

5.2. In their reply, the controller stated the following:

i. The data breach was deemed is likely to result in a high risk to the rights and freedoms of the affected data subjects. Moreover, the controller chose to inform their registered users through the website blog post taking into consideration:
    - That there was no indication of how many and which users were affected by the breach and
    - the very large number of registered emails which would take approximately 5 months to inform by individual emails.

ii. As regards the identification documents requested,
   - the procedure for requesting identification documents is only for data subject access requests,
   - the purpose is to protect user data from unauthorized disclosure,
   - the identification documents are deleted after verifying the identity,
   - the email address is not a sufficient security measure,
   - the identity is authenticated by comparing the identification document with existing records or billing information,
   - the procedure follows the GDPR requirement of using reasonable measures to verify the identity of the data subject (Recital 64 GDPR).

iii. The complainant's access request was considered as satisfied since the controller provided all the necessary information and explanations with regards to the account opened under his email address as well as all the information that could be provided about the incident.

5.3. The Commissioner's Office took into account the above facts and information, the comments from concerned supervisory authorities, and noted the below:

i. It was considered that a blog post was not sufficient for the communication of the data breach to the affected data subjects and thus the Commissioner immediately instructed the controller to proceed with sending an email to all registered users regardless of the effort and time needed. The controller complied with the instruction without delay.

ii. The account registered to the complainant's email address was active and thus the erasure of the data was not justified before the complainant contacted them.

iii. The registration process requires that the user confirms the registration by using a single-use password that is sent to his mailbox thus ensuring accountability.

iv. The complainant's email address was confirmed during the registration, which could only be done by a person with access to the specific email address. Considering that the complainant claims he did not perform the registration himself, it can be deduced that his email address was accessed by a non-authorized person.

v. When the complainant informed the controller that someone else used his email address to register, the controller informed him that in this case, the Username and IP address were personal data of the third party who opened the account by using his email address. Moreover, the complainant was informed about what type of data were related to the account associated with his email address and was also informed that the account and the connected personal data would be deleted from the website database since the account was fraudulently opened.

Preliminary Decision

6. On 15 June 2023, the Commissioner issued a Preliminary Decision regarding the above investigation. In the said Preliminary Decision, the Commissioner concluded that:

a. The complainant's account was active and the controller was not aware that it was opened fraudulently. Therefore, the controller had no reason to erase the data before the incident.
b. There is **a breach of Article 5(1)(c) GDPR** (principle of data minimization) since the controller did not have a plausible reason to ask for a government ID from the complainant, specifically considering that:
    i. the controller requested the identification before they were notified by the complainant that the account was opened fraudulently,
    ii. the controller could not have used any government ID to identify the DS, since the controller does not already process any of the data types included in any government issued ID,
    iii. the complainant could have been identified through the linked email address without the need for additional identification documentation, and
c. there is **an infringement of Article 34(1) GDPR** since the controller did not communicate the personal data breach in an appropriate way.

7.1. The controller responded on 26 June 2023 to the Preliminary Decision and stated, inter alia, that:

a. The company has implemented further organizational and technical measures to guarantee full compliance with the GDPR.
b. With regards to the infringement identified under Article 5(1)(c) of the GDPR, the collection of identification documents procedure was only applicable to "access requests" and the intention was strictly to protect the data of the users from any unauthorized disclosure in accordance with Recital 64 of the GDPR. Nevertheless, this procedure has been abandoned and the email verification will be used as a sufficient measure to verify the ownership of the personal data in question.
c. With regards to the infringement identified under Article 34(1), at that time it was considered the public announcement through the website blog was the most suitable and efficient measure to inform the affected users. In addition, the process of contacting each user personally through an email would have taken at least 5 months to be completed in comparison with the mass and immediate notice through the blog. Despite this, the controller complied with the Commissioner's instructions and proceeded with personal email notification as it was not their intention to avoid informing the affected users.

7.2. In addition to the above, the controller included the following mitigating factors to be taken into account by the Commissioner:

a. The controller immediately informed the Commissioner about the incident and took all reasonable steps to mitigate the impact on its users. In

addition, it was and as of today is still in constant communication with the Commissioner.

b. Even though the company has been operating since 2016, it is the first time that the Commissioner or any other DPA authority receives a complaint about the company procedures regarding GDPR.
c. The controller complied with all the requests of the Office of the Commissioner for Personal Data Protection without any delay and consulted the Commissioner during all steps to ensure compliance with GDPR.
d. Actively improved its security measures and internal processes as per the guidance and recommendations of the Commissioner. It informed its users through direct email communication in addition to the public announcement initially made and changed its procedure regarding the access requests of the data subjects.
e. It is clearly evidenced from its immediate compliance with the Commissioner's requests that there was no intention to infringe either article 5(1)(c) or article 34(1) of the GDPR.

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 34(1) of the GDPR** *"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."*

8.3. **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;

8.4. **Recital 86 of the GDPR** states that *the need to mitigate an immediate risk of damage would call for prompt communication with data subjects.*

Views of the Commissioner

9. Following the above facts and the response to my Preliminary DecisionI note the below:

9.1. I recognise that the controller's intention for requesting an identification document was to protect any unauthorized disclosure. Despite this, as it is stated in recital 64, *a controller should not retain personal data for the sole purpose of being able to react to potential requests.* Thus, collecting identification documents solely for satisfying data subject rights is excessive, regardless of when the data is collected.

9.2. Additionally, I hold the position that the controller should have informed the affected data subjects more directly taking into consideration the nature of the breach and the categories of personal data affected. This is also strengthened by the fact that the controller regularly processes data concerning the sex life of its registered users.

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 by Technius Ltd of **Article 5(1)(c) and 34(1)** of the GDPR, for the reasons mentioned above.

11. Moreover, following an infringement of Article 5(1)(c) and 34(1) 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.
2. The controller complied with all the requests of the Commissioner without any delay.
3. The measures taken after the incident to ensure that all staff is appropriately trained in handling GDPR matters.
4. The controller should have taken appropriate and prompt measures in effectively communicating the breach to its users.
5. The complainant should have been identified using other less excessive means.
6. The controller should have implemented more appropriate procedures and measures considering the processing of special categories of data.

14. 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 Technius Ltd for the infringement mentioned in paragraph 10 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

REPUBLIC OF CYPRUS

OFFICE OF THE COMMISSIONER
FOR PERSONAL DATA
PROTECTION

COMMISSIONER

Our ref.: 11.17.001.010.172

23 October 2023

Decision

Investigation of complaint under the General Data Protection Regulation (GDPR)

A complaint was lodged with the Malta DPA against Brivio Limited (hereinafter, "the Controller"), a company that is registered in Cyprus. The complaint was subsequently transmitted to the Office of the Commissioner for Personal Data Protection (hereinafter, "the Commissioner's Office") on 16/06/2022, in line with Article 56 of the General Data Protection Regulation (EU) 2016/679 (hereinafter, "the GDPR").

2. On the basis of the above, the Commissioner for Personal Data Protection (hereinafter, "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 was lodged by [redacted] (hereinafter, "the Complainant") and involves the Controller's failure to comply with the Complainant's access request (Article 15 of the GDPR). The complaint included the following information:

3.2. The Complainant, who is a registered user on the online casino "icecasino.com" (hereinafter, "the website"), contacted the Controller, who is the operator of the said website via email at support@icecasino.com on 22.02.2022, requesting that he is provided with information regarding all personal data concerning him, payments made and casino games that he has participated in on the website as is his legal right according to Article 15 of the GDPR. Nevertheless, the Complainant claims that he had not received a response to his request within the one-month period pursuant to the Article 12(3) and (4) of the GDPR.

Investigation by Cyprus SA

4.1. The Commissioner's Office contacted the Controller on 05/09/2022 and requested the reason for not responding to the Complainant's access request as well as any other information they deemed necessary. The Controller was also informed for the provisions of the Article 12(3) and (4) of the GDPR.

4.2. In their reply, on 19/09/2022, the controller stated the following:

i. On 22.02.2022, the Customer Support Team (email support@icecasino.com) received an email from the Complainant requesting that they provide the latter with

information regarding all personal data concerning him, including payments made and casino games that he had participated in.

ii. In course of the Controller's internal investigation, it ascertained that despite the internal data protection policies and procedures of the Controller, the Customer Support employee failed to inform the Data Protection Team regarding this particular request.

iii. Taking into account the specifics of their business and to limit employees' access to the customers' personal data, they have intentionally designated a separate team for privacy matters. Therefore, their customers are always encouraged to contact the Data Protection Team directly at privacy@icecasino.com in case of questions, requests, or complaints. Nevertheless, following the GDPR, the Controller mentions that they accept data protection requests via all available means of communication, and all the staff interacting with customers are instructed on how to reply to different types of data subject requests.

4.3. Moreover, to effectively deal with this case and enhance internal technical and organisational measures imposed by the GDPR to be in a position to reply to all demands in a timely manner, the Controller informed the Commissioner's Office that several corrective actions were applied:

i. When the Data Protection Team received the complaint, they immediately contacted the Complainant and, on 12.09.2022, the personal data were sent to the latter. Therefore, the subject access request has been fully satisfied. The Malta SA confirmed that, on 24/11/2022, the Complainant access request was indeed fully satisfied.

ii. The privacy procedures have been reviewed and a new technical flow has been adopted in order to facilitate the cooperation between the Customer Support Team and the Data Protection Team and to ensure that all data subject requests are answered in a timely manner in the future.

iii. Additional training sessions have been conducted, for the staff who interacts with customers and instructions have been granulated as to how the staff should reply to each type of request.

4.4. As requested by the Commissioner's office, the Controller provided the former, on 25.11.2022, with the following written evidence of the corrective measures taken:

i. The Subject Access Request Procedure

ii. Screenshots of the information system where data subject requests are processed

iii. The educational content of the course on 'Privacy and Customer Service' which all members of the Customer Support Team were obliged to complete, as well as proof of completion by the staff.

4.5. Furthermore, the Controller informed the Commissioner's office about the updated workflow, according to which, the members of the Customer Support Team, immediately after receiving the data subject request, they recognize and identify the data subject request among other messages, ask security questions to verify the data subject identity, create a service ticket in the information system and assign a service ticket to the Data Protection Team. After that, the Data Protection Team takes all the necessary actions to implement the data subject's rights in a timely manner.

Preliminary Decision

5.1. On 06/07/2023, the Commissioner issued a Preliminary Decision and concluded that:

i. There is an infringement of the Article 12(3) of the GDPR, since the Controller failed to satisfy the Complainant's access request and comply with the provisions of the aforementioned Article.

ii. The Controller's immediate actions to satisfy the access request, as well as the corrective measures taken after receiving notice for the complaint, are taken into consideration.

iii. It is worth mentioning that a similar complaint against the Controller had been lodged to the Austria SA and thereafter received by the Commissioner's office. The complaint was referred to the Controller's failure to respond to an access request exercised by an attorney on behalf of a data subject, since no additional information was requested to assure that the said attorney was entitled to represent the data subject. Considering the fact that the Controller eventually complied with the access request, the Commissioner was of the view that the mere delay appears to be a minor infringement which only slightly affected the data subject's rights and freedoms. Therefore, the Commissioner considered that the investigation proceedings could be concluded as no further supervisory measure was necessary at that stage. The information about the case conclusion was sent to the Controller on 05.01.2023.

5.2. The Commissioner invited the Controller, as by 03/08/2023 at the latest, to state the reasons why they believe they should not be sanctioned and/or any mitigating factors that they believe should be taken into account before a Decision was issued.

5.3. On the 07/07/2023, the Controller informed the Commissioner that they would answer within the set period. However, the Commissioner sent a reminder, on 04/09/2023, since no such response was received within the deadline.

5.4. The Controller responded on 04/09/2023 to the Preliminary Decision and stated, inter alia, the following:

i. <u>The Complainant's right to access was completely fulfilled.</u>
Despite the initial delay in responding to the Complainant, upon becoming aware of the request, the Controller promptly reached out to the Complainant and completely fulfilled their request. Consequently, the former actively played a role in mitigating the effects of delayed response on the latter's rights and freedoms. By successfully fulfilling the Complainant's access rights, the Controller did their best in these circumstances to effectively meet the objectives of Article 15 of the GDPR. The Complainant, upon receiving the comprehensive response to their request, did not assert any claims concerning their data protection rights. The Controller believes that this demonstrates the effectiveness of their efforts in addressing the situation promptly and thoroughly, and they consider the matter to be resolved to the satisfaction of the Complainant. They believe that the essence of data protection regulations is to safeguard the rights and freedoms of individuals, and in this case the Complainant's rights were protected and their request fulfilled.

ii. The Controller enhanced their internal policies and procedures concerning data subject rights.

To ensure timely responses to data subject requests, the Controller has introduced a range of corrective measures, encompassing both organisational and technical improvements. Such measures include:

- revision of the Subject Access Request Procedure and update of the company's workflow concerning the data subject requests;
- setting up a new technical flow for cooperation between the Customer Support Team and the Data Protection Team;
- improvement of internal compliance training 'Privacy and Customer Service' mandatory for all members of the Customer Support Team;
- conducting additional training sessions for the staff interacting with the customers, to remind them of the privacy policies and procedures.

Due to these improvements, the Controller successfully avert delays in responding to data subject requests, ensuring compliance with Article 12(3) of the GDPR.

iii. The Controller actively cooperated with the Commission throughout the investigation process.

Demonstrating openness and transparency, the Controller provided the Commission with comprehensive explanations regarding the case, along with supporting evidence of the corrective measures implemented. Thus, the Controller contributed to an effective investigation through every available means. Considering all mentioned above, they believe that in this case, holding the company accountable is excessively burdensome and disproportionate, taking into account the fact that the resolution of the matter left the Complainant satisfied, and given the company's endeavors to remain compliant with the GDPR and transparent with the Commission throughout the investigation process.

Legal framework

6.1. Article 58 of the GDPR:

"1. Each supervisory authority shall have all of the following investigative powers:
(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; [...]

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the 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 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; [...]

(f) to impose a temporary or definitive limitation including a ban on processing; [...]

(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; [...]"

6.2. Article 15 of the 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. [...]

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".

6.3. 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. [...]"

Views of the Commissioner

7.1. After reviewing the information provided by the Controller, in their response to my Preliminary Decision, I consider the following:

7.2. Regarding what the Controller states, in paragraph 5.4.i. above, I take into consideration that the Controller promptly reached out to the Complainant and completely fulfilled their request. Nevertheless, I consider that, the Controller understands that the request could have been satisfied from the first instance if the appropriate organizational and technical measures were in place and the staff was properly trained in dealing with GDPR requests in a timely manner.

7.3. Moreover, regarding the claims of the Controller that, the Complainant, upon receiving the comprehensive response to their request, did not assert any claims concerning their data protection rights and that the resolution of the matter left the Complainant satisfied, I would like to point out that, the Data Protection Team got aware of the access request and the Controller satisfy the request, after the Complainant lodged a complaint with my Office.

7.4. As for the corrective measures, mentioned in paragraph 5.4.ii. above, which the Controller has taken in order to be in a position to reply all demands in a timely manner, are also favorably considered.

7.5. Regarding the paragraph 5.4.iii. above, I understand that, by the term "Commission", the Controller means my Office. Consequently, I accept the claim of the Controller that they actively cooperated with my Office throughout the investigation process, despite the fact that, they had not responded to the Preliminary Decision in a timely manner.

Decision

8.1. In the view of all the above facts, I find that there is a violation of the Article 12(3) of the GDPR, for the reasons mentioned above.

8.2. Considering both the following moderating (a-d) and aggravating (e-h) factors:

a. the eventual and prompt satisfaction of the access request;
b. the corrective measures taken regarding the handling of data subject requests;
c. the Controller's cooperation in the investigation process;
d. the minor infringement on the Complainant's rights and freedoms;
e. the Controller's Data Protection Team only became aware of the access request after being notified of the complaint by my Office;
f. the non-satisfaction of the access request according to the Article 12(3);
g. the non-existence of appropriate measures in order to deal with GDPR requests in a timely manner;
h. the existence of a previous similar violation by the Controller;

and based on the corrective powers granted to me according to the Article 58(2) of the GDPR, including *"(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation"*,

the Commissioner decided to issue a reprimand to Brivio Limited to ensure that in the future it handles the data subject rights in accordance with the provisions of the Article 12(3).

8.3. It is understood that in case of a similar incident, this will be handled more strictly and the present complaint will be taken into consideration on taking any supervisory measures.

Commissioner
For Personal Data Protection

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

UOOUX00DULVQ

Ref. UOOU-00776/21-6

RESOLUTION

The Office for Personal Data Protection (hereinafter "the Office"), in its capacity of the competent administrative authority pursuant to Article 64(1) of the Act No. 110/2019 Coll., on personal data processing, and to Article 58(1)(d) of the 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), has decided on 17 May 2021 as follows:

The case concerning the suspected company [redacted] company identification number [redacted] established at [redacted] which allegedly have committed an offence pursuant to Article 62(1)(c) of the Act No. 110/2019 Coll., on personal data processing. The company, despite a request from [redacted] of 17 March 2020 for erasure of his personal data, contacted him anew on 4 May 2020 via e-mail containing yet another marketing communication. The company, by this action, has allegedly breached the data subject´s rights laid down in Article 17(1)(c) of the Regulation (EU) 2016/679, specifically the right obliging the controller to erase personal data without undue delay concerning the data subject, if this particular data subject objects to the processing pursuant to Articles 21(1) and 21(2),

is pursuant to Article 65 of the Act No. 110/2019 Coll., on personal data processing, **discontinued the proceedings.**

Reasoning:

The Office received on 17 January 2021 via the IMI system, a complaint lodged originally with the Office for Personal Data Protection of the Slovak Republic by [redacted] concerning an unlawful processing of his personal data in relation to sending of marketing communications. The complainant stated in his complaint of 5 May 2020 that he, on a not-specified day, made an order for goods at the e-shop [redacted] On 17 May 2020, at 17:29 hrs, he obtained an e-mail message from the customer service of this e-shop informing him that the ordered item was dispatched to him on 16 May 2020. On the same day, the complainant received a letter from the e-shop [redacted] file number [redacted] signed by [redacted] informing him that the ordered item was sold out and the order could not be accommodated. With regard to these two contradicting

pieces of information the complainant had lost confidence in the given e-shop and had withdrawn his order on the very same day at 20:13 hrs and simultaneously asked for erasure of his personal data provided to the company in relation with the order. He sent the request for the order withdrawal as well as for the erasure of his personal data to the customer service to the e-mail address [redacted] He backed his statements by a copy of the given e-mail communication. On 20 March 2020 the complainant received an answer form the customer service, sent from the address [redacted] saying that the company respected his wishes and would refrain from any sending of offers. The company added further that database of offers was set up in advance, i.e. it was created yet before the complainant´s request for erasure was filed. The company also apologized for the case, if still the complainant would in the coming days obtain a marketing offer. Despite the complainant´s request for erasure, the suspected company sent him electronically marketing offers of the e-shop [redacted] whereas the last offer was sent by e-mail on 4 May 2020 at 12:38 hrs. A copy of the marketing offer was attached as well.

As per Article 21(2) of the Regulation (EU) 2016/679, 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, which includes profiling to the extent that it is related to such direct marketing. Pursuant to paragraph 3 of the mentioned article, where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. Pursuant to Article 12(3) of the Regulation (EU) 2016/679, 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. However, also in this case, the controller shall inform the data subject of such extension within one month of receipt of the request.

With regard to the aforementioned facts, the administrative authority asked on 15 April 2021 the suspected company for cooperation in accordance with Article 31 of the Regulation (EU) 2016/679 and requested the processor´s agreement with the company [redacted], established at [redacted] Slovak Republic, company identification number [redacted] which provides to the e-shop [redacted] the customer service. The administrative authority also asked, when the suspected company was informed of the complainant´s request for erasure of his personal data and what measures the suspected company had taken in relation to the complainant´s request.

In reaction to its request, the administrative authority received on 28 April 2021 a statement in which the suspected company explained that the request for erasure of personal data, or, respectively, the discontinuation of sending of the commercial offers to [redacted] from the e-mail address [redacted] was obtained on 17 March 2020, whereas on 20 March 2020 the [redacted] operator entered this request to the system for further handling. On 27 May 2020 the physical removal of the complainant´s personal data from the direct marketing database took place. The suspected company stated further that it was discovered during a checkback that yet, several marketing communications were sent to the complainant due to a technical mistake within the system.

The suspected company also stated that after in relation to this failure, it had conducted a revision of the entire process and applied measures preventing repetition of similar mistake.

Moreover, the suspected company informed that customer data are processed over the period covering the order processing plus delivery and subsequently also over periods related to the warranty claims purposes as well as periods during which buyers may apply their claims or a competent supervisory body could perform an inspection. Following the suspected company, these personal data are processed on legal grounds for the purposes of observing an agreement and of the suspected company´s legal interests, however not longer than for three years as of the filing of an order. The information for customers as to the processing of personal data are available at the website [redacted] In relation to the complainant´s request, the company stated that his personal data had been removed from the demarketing database, but it could not erase all personal data as they were processed in connection with his order on the basis of a legal interest of the suspected company whereas they should be erased automatically after three years as of the filing of the order.

The suspected company also attached the agreement on processing of personal data closed on 25 May 2018 with the company [redacted] which provides for the suspected company customer service. It also attached the processor´s technical and organizational measures of 25 May 2018 as well as a sample of the electronic newsletter footer where a customer may unsubscribe reception of electronic newsletters. Finally, the invoice and the delivery confirmation related to the complainant´s order was attached.

The administrative authority has assessed the suspected company´s conduct and declares that the suspected company, after the complainant´s sending of his request for erasure of 17 March 2020, removed on 20 March 2020 the complainant´s personal data from its marketing distribution list and informed him thereof by e-mail on the same day. The suspected company could not accommodate the complainant´s request for erasure of his personal data due to the fact that the formerly closed agreement related to the complainant´s order is subject to Article 6(1) of the Regulation (EU) 2016/679 as they are necessary for compliance with the suspected company´s legal obligations and for the purposes of its legal interests. Due to a technical failure on the suspected company´s side, marketing offers (catalogue and newsletter) were sent to the complainant even after his personal data had been removed from the distribution list, whereas subsequently the suspected company took measures preventing repetition of such an event.

On the basis of the material collected in the file, the administrative authority, in accordance with Article 65 of the Act No. 110/2019 Coll., discontinued the proceedings without initiating proceedings concerning an infraction as only a single mistake occurred on the suspected company´s side and with respect to the significance and extent of the breach of the protected interest that was affected by the action and also with regard to the conduct of the suspected company that, immediately after the case happened, it remedied the unlawful situation. It is obvious that the objective that could have been achieved by performing a proceeding, was reached even so.

Instruction: This resolution shall, pursuant Article 65 of the Act No. 110/2019 Coll., only be recorded in the file. In accordance with Article 76(5) of the Administrative Code, this resolution cannot be appealed.

Prague, 17 May 2021

[redacted]

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

UOOUX00F1SE9

Ref. UOOU-04603/21-1
Prague, 4 November 2021

Official record on handling of a complaint

The Office for Personal Data Protection (hereinafter "the Office") received on 15 February 2021 from the German supervisory authority, via the IMI system, a complaint by a German citizen against the conduct of the company [redacted], established at [redacted] Czech Republic, company registration number [redacted]. Pursuant to the complainant, the company requires for the activation of the unlock/lock-up functionality of a [redacted] car, through the [redacted] application/service, for the purpose of identity check of the person asking for the service activation, a copy of the driving licence even if it already possesses the identity card´s number of the person who has purchased that [redacted] car.
[redacted] conveyed to the German supervisory authority the information that the controller of customer data in connection with the operation of the [redacted] application is the company [redacted], established at: [redacted] company registration number [redacted] (hereinafter "the Company" or [redacted] .
The German citizen´s complaint, bearing characteristics of a transborder processing, has been passed on to the Office as the competent authority for further handling.

The Office, within its competences vested by Article 31 of the 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 "the Regulation (EU) 2016/679") as well as in connection with Article 50(1) of the Act No. 110/2019 Coll., on personal data processing, asked on 30 March 2021 and repeatedly on 14 April 2021 the Company for statement as to the ownership of the [redacted] application accompanied with a detailed description of the customer activation procedure and for the provision of the relevant documentation.

The following information were particularly requested:

1) *Who is the owner of the [redacted] application? Does the company [redacted] use this application for its business activity and if so, in what manner? Please specify precisely.*
2) *Please describy the entire customer activation procedure of the [redacted] application and provide as evidence the relevant documentation.*

3) *Do you require a driving licence copy for the activation of the unlock/lock-up functionality via the [redacted] application?*
   a. *If yes, are these copies or scans filed and retained by the company [redacted]? In what file?*
   b. *For how long?*
   c. *What software is used for the retention of these documents? (convey precise information including certificates and provider)*
   d. *If, for the activation of the unlock/lock-up functionality via the [redacted] application, a copy of some other proof of identity is required, provide information as to what kind of proof is required and reply the questions under 3.a) thru 3.c).*
4) *Provide and evidence the extent of personal data processed by [redacted] through the [redacted] application.*
5) *Provide the legal grounds pursuant to the Regulation (EU) 2016/679 on the basis of which [redacted] processes personal data of its customers via the [redacted] application;*
   a. *If the legal title laid down in Article 6(1)(f) of the Regulation (EU) 2016/679 is at stake, submit also the balance tests;*
   b. *If the personal data are processed on the basis of Article 6(1)(a) of the Regulation (EU) 2016/679, please document how the consent is obtained;*
6) *If [redacted] engages a processor for the processing of personal data within the [redacted] application in accordance with Article 28(3) of the Regulation (EU) 2016/679, provide contracts related to these processing operations;*
7) *Provide, in compliance with Article 30 of the Regulation (EU) 2016/679, records of processing activities related to the personal data treated via the [redacted] application;*
8) *Submit technical and organizational measures pursuant Article 32 of the Regulation (EU) 2016/679 adopted for the security of personal data processed via the [redacted] application including technical specifications and certificates.*

To verify the Company´s statement and the real-life practice in this respect, the [redacted] car dealer [redacted], respectively [redacted] company registration number [redacted] was asked on 9 September 2021 for explanation about the [redacted] application. Specifically, it was enquired about the process of activation of the [redacted] application, the agreement with the controller (the Company), the extent and method of customer data collection during the activation of the [redacted] application with special focus to the identity checks of customers.

The following information was particularly sought:

1) *A copy of the data processing agreement between [redacted] a.s. and [redacted].*
2) *A comprehensive description of the entire process of activation of the [redacted] application including the establishment of the ID [redacted] account for needs of the customers. Submit particularly documents evidencing the method of customer data entry and the extent thereof (e.g. PrintScreen of each specific step, work procedure/employee manual).*
3) *Provide the legal title pursuant to the Regulation (EU) 2016/679 your company applies for the processing of customer data via the ID [redacted] and the [redacted] application.*

4) *Submit copy of guidance and work procedures provided by [redacted] to the [redacted] car dealers for the purposes of ID [redacted] account establishment and the activation of the [redacted] application.*
5) *Specifically, provide information, if [redacted] requires a copy of the customer´s driving licence in order to establish the ID [redacted] account and to activate the [redacted] application.*

I.

The information and documentation obtained from [redacted] concerning the customer data processing in relation to the service provision agreements reveal the following:
The condition for profiting from the Company´s services is creation and application of the central user account [redacted] ID, i.e. the identity for the customer single sign-in to the [redacted] online environment. The [redacted] ID functionality serves to the customer identity check on the basis of the customer´s personal ID (driving licence). The verified customer can then use the [redacted] services. The identity of a verified customer enables to use the Service advisor, Service technician, Service assistant, Sale services staffer, Head of new cars sales, New cars sales staffer and Head of used cars sales.
[redacted] recommends verifying the customer identity during the car service under the customer´s presence (validity of the personal data and car-related data processed).

[redacted] ID functions as single identity within the [redacted] environment. The customer registration within one environment is enough then to start using other services that [redacted] offers or will offer in future.
Conditions of the [redacted] ID usage on the legal grounds pursuant to Article 6(1)(b) of the Regulation (EU) 2016/679 and information on the customer data processing are, in sense of Article 12 et all. of the Regulation (EU) 2016/679, are presented to the customer upon the car purchase and are also publicly accessible on the [redacted] website [redacted], that contain links to the privacy policy, cookies and also the standalone [redacted] service, for the activation of which it is necessary to close online separate agreement with the Company [redacted] Contact to the data protection officer is provided there as well: [redacted].

The process of signing on to the [redacted] services:
After entering the [redacted] online environment, the customer signs on by using the [redacted] ID whereby the registration process is initiated.
Upon opening the [redacted] account, the customer is transparently made acquainted with the "Conditions for using [redacted]" and the "Information on personal data processing". These documents are part of the information provided at time of the online sign-on to the [redacted] services and are publicly accessible on the Company´s website as well.
After establishing the [redacted] user account by a customer, a step follows that match the vehicle (by entering the VIN code) with the [redacted] user account. Entering (by the customer) of the generated code into the car infotainment follows. After this security step, the car is "parked in the virtual garage" provided by the [redacted] account and the customer is enabled to profit from the services contracted.

The electronic processing of customer data is, pursuant to the commercial terms, based on the free decision of the customer to contract paid [redacted] services (first order for services linked to a new car is free of charge).
The online contract with the Company related to the [redacted] services related to one vehicle is concluded in the sense of Article 6(1)(b) of the Regulation (EU) 2016/679.
The period of the contractual relationship is set for three, or for more years. If car user, the customer can cancel the service order without providing any reasons within 14 days as from its conclusion.
The [redacted] services can be used via:

- Infotainment equipped with a system directly from production;
- Management unit of the e-call system enabled also for the mobile apps of the online service;
- Webpages of the [redacted] service;
- Mobile app.

Usage of certain [redacted] online services is for security reasons subjected to the customer identity check at the Company´s authorized partner on the basis of driving licence. For instance, [redacted] is a service from the category marked as II. [redacted] *"Unlock and lock up" (the customer can remotely, via the portal or a mobile app lock up or unlock a particular car. For the service activation, it is necessary that an authorized* [redacted] *partner verifies the customer´s identity)*.

The Company processes customer data for the purpose of closing a contract on provision of the [redacted] mobile online services, whereas the provision of customer data is a contractual condition. Refusal to provide these personal data may result in the non-conclusion of the agreement.
Processing of customer data required by the Company in relation to the [redacted] online service is thus realized for the purpose of the contract performance pursuant to Article 6(1)(b) of the Regulation (EU) 2016/679, whereas the extent of the data processed (driving licence number, issuing country and date of expiry) is, in sense of Article 5(1)(c) of the Regulation (EU) 2016/679, adequate, relevant and limited to what is necessary in relation to the purposes and meets the security role of preventing the customer´s car from misuse in relation to the false usage of the [redacted] service by an unauthorized person, *for instance, the remote unlocking and locking up of the vehicle.*

The contract performance is conditioned by the active acceptance of the "Conditions of [redacted] ID application", whereby the customer may refuse the provision of the [redacted] services and use the [redacted] car without these services. The possibility to use the whole scope of these services is dependent on the particular car´s equipment as well as on the specification of services that the customer contracted with [redacted].

The company [redacted] is in sense of Article 4(7) of the Regulation (EU) 2016/679 the data controller as well as the owner and operator of the [redacted] application that can be used only with the use of publicly available communication technologies. The application is equipped with the so-called "connective services" that connect the vehicle with its authorized user. The online infotainment means an interactive solution of breakdowns and problems with

the car or the remote access to the information about the car condition, remote unlocking and locking up, etc.

[redacted] stores customer data in the sense of the processing agreement *"Agreement on protection of personal data for the purpose of compliance with the Regulation (EU) 2016/679 (GDPR) with regard to custom-performed processing of personal data"* with the data processor which is the company [redacted] in Germany, agreement number: [redacted]. [redacted] is in position of a processor in sense of Article 4(8) of the Regulation (EU) 2016/679.
Both [redacted] and [redacted] are part of the [redacted]

It is clear from the documents and the written statement by [redacted] that the company **does not require from its customers copy of the driving licence**, but processes, in order to ensure the [redacted] services ordered by the customer (for security reasons to oversight the [redacted] ID system) data entered in the driving licence: number of the licence, date and country of issuance, expiry date. The driving licence number is entered into the system online by the customer, or on the customer´s request by the authorized dealer or service at time of the [redacted] ID or [redacted] activation.

„Dealers may at time of the car handover proof the identity of the customer for the purposes of activation of some security-relevant [redacted] services by checking the name, surname and date of birth displayed on the customer´s driving licence and compare them with the data provided by the customer upon the registration with [redacted] ID, respectively [redacted]. Or, as the case may be for security, to the end of performance of the [redacted] agreement (remote unlocking and locking up of the car) enters into the system the driving licence number, date and country of issuance and the expiry date.
Dealers are legal persons on their own on the basis of business contracts and possess all necessary documents concerning processing of personal data circulating among [redacted] and the dealer network."
[redacted] provides to the dealer network a detailed guidance how to proceed during the customer identity check for the purposes of [redacted]. A customer is regarded as proven if the driving licence number, country of issuance and its expiration has already been entered into the system. A customer that has not been verified cannot get the "unlock and lock-up service" activated for security reasons (Documented by file [redacted]).

The submissions from [redacted] are filed under ref. [redacted].

II.

The [redacted] statement was verified with the [redacted] dealer [redacted], company registration number [redacted] (hereinafter [redacted]).
Concerning activation of the [redacted] [redacted] application, the Office received the following information:

[redacted] has closed an Agreement on processing of personal data with the data controller [redacted] and provides, within its business activity, for the [redacted] car owner also other services from [redacted] among others the registration with [redacted] ID, and [redacted]

[redacted] respectively. Consequently, [redacted] is in the position of a processor in the sense of Article 4(8) of the Regulation (EU) 2016/679.

[redacted] has confirmed the [redacted] statement that the creation of a [redacted] ID account and its activation is done by the customer itself and that for its opening it is not necessary to provide a driving licence copy.
The activation of the [redacted] application is done by the customer as well. The manual (Brochure titled [redacted] on-line services) how to proceed is given to the customer at time of a binding order of a car. The customer, with help of the manual, activates access to the [redacted] service. Later, upon the handover of the new car and upon the customer´s request, the dealer helps the customer with the sign-on into the [redacted] ID environment and with the activation of [redacted] service in the vehicle. The sign-in and the service activation is performed with the access data which the customer itself has activated.
In case the customer decides to use some of the extended [redacted] [redacted] services (e.g. remote unlock/lock-up), the identity is checked exclusively under the customer´s physical presence at the dealer´s.The customer verification process is performed in accordance with the relevant methodology, the [redacted] The customer´s identity is checked via the personal ID (driving licence).
Any copy of driving licence for verification of the customer identity, neither durin the [redacted] activation, is not requested pursuant the methodology and the information conveyed by an [redacted] representative.

It was found out and back checked that [redacted] a.s. provides its customers the service called [redacted] on the basis of a contract (e.g. remote unlocking/locking up of the car) and processes in this regard customer data in sense of Article (6)(1)(b) of the Regulation (EU) 2016/679. For the purpose of an enhanced security, the processed data include also the [redacted] licence number (and country of issuance and expiry date) which is entered into the [redacted] ID system and (as the case may be) to the [redacted] system and serve to the identity verification of a customer requiring the service (e.g. remote unlocking/locking up of the car).

It shall be stated, on the basis of the aforementioned findings, that [redacted] does not require copy driving licences. Dealers can offer their customers help during the activation of the [redacted] application, but neither they are authorized to require a copy of driving licence from customers.
The German customer´s claim that [redacted] requires for the activation of the [redacted] application a driving licence copy has not been proven.

The supporting documents from the [redacted] car dealer in the Czech Republic, the company [redacted] are filed under the reference [redacted]

Summary:

It has not been found out on the Czech Republic´s territory that [redacted] or its authorized dealer requested a copy of driving licence for the purpose of activation of the agreement relating to [redacted].

On the contrary, the Company has provided evidence that it has not requested any driving licence copies for the activation of the [redacted] services, the registration with which is done online and upon the customer´s request.
Moreover, for the provision of additionally contracted services of [redacted], again on the customer´s request (e.g. the service of remote unlocking and locking-up), [redacted] requires electronic processing of the driving licence number, country of issuance and date of expiration. These data are transferred electronically to the Company by the customer itself whereas an authorized [redacted] representative may help him upon request. The transfer of these data by the customer is voluntary, but it is a condition for the provision of the requested [redacted] services.
At time of the activation of this service, an authorized [redacted] representative does verify on spot the customer´s identity on the basis of the personal data stored in the system and the physically presented driving licence.
It is an electronically closed contract concerning the provision of services between [redacted] and the customer in sense of Article 6(1)(b) of the Regulation (EU) 2016/679.

The company [redacted] does not require from customers for the activation of the [redacted] service any copy of driving licence and it has been concluded that the company´s procedure did not fall under Article 4(7) and 4(8), Article 5, Article 6(1)(b), Artcile (12) and other following Articles of the Regulation (EU) 2016/679, and consequently, no breach of the relevant legal obligation has been detected.

The complainant failed to document his claim that [redacted], a.s. would allegedly have required copy of driving licences from the authorized dealers in Germany for the purpose of their processing for the activation of the [redacted] service. Therefore, the Office considers that the merit of complaint shows an individual wrongdoing by am authorized company in Germany which required a driving licence copy for the activation of the remote service of unlocking and locking up of a vehicle.

In accordance with the Regulation (EU) 2016/679 and the Act No. 110/2019 Coll. on processing of personal data, the complaint towards the company [redacted] has been adjourned, as there is no reasoned suspicion as to the breach of legal regulations, neither of regulations specifically related to the protection of personal data, nor of other regulations. Therefore, the content of the complaint has not been found reasonable as to the launch of an investigation or commencement of administrative proceedings whilst it would not be appropriate to settle the matter in other way.
Any further Office´s proceeding would not open the possibility to find out further facts that could support any conclusion other than the one described in this official record.

The German supervisory authority will be informed of the outcome of this case through the IMI system.

[redacted]
(signed electronically)

Our reference: LDA-1085.1-2993/22-F
IMI Art. 56: 399988
IMI draft decision: 538804

INOFFICIAL TRANSLATION

Controller: [redacted]

On the basis of the draft decision of the National Data Protection Commission Luxembourg (CNPD) No. 538804, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) pursuant to Article 60(8) of the GDPR issues the following

Final Decision:

The complaint is rejected.

Justification:

I. Facts

The complaint was received by the BayLDA on 9 April 2022 and was forwarded via IMI to the CNPD as the lead data protection supervisory authority for the controller.

In his complaint, the complainant stated that he is a client of the controller. The latter transmitted his personal data to a service provider unknown to him, without a basis in data protection law.
He concluded this as he had been contacted by telephone on 16 March 2022 by that service provider. The caller knew personal data relating to the complainant's identity and his business relationship with the controller.

The CNPD concluded that the complainant requested a review of the lawfulness of the processing in accordance with Articles 5 and 6 of the GDPR.

In accordance with Article 57(1)(f) of the 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 the lawfulness of the processing.

In the course of those investigations, the CNPD received the following explanations from the controller in due time:

a. By letter of 2 December 2021, the controller (an online bank distributing credit cards and insurance products) sent the complainant an invitation to participate in a raffle.

b. On 21 December 2021, the complainant stated that he wished to participate in this raffle and gave his consent to be contacted by e-mail, SMS and telephone for advertising purposes.

c. On 16 March 2022, the complainant as part of a marketing campaign concerning the controller's 'Payment Protection Insurance' product was contacted by the company [redacted], which provides and advertises this product on the German market for the controller.

d. On 26 March 2022, the complainant asked the controller to explain when he had given his consent in this regard.

e. In his reply of 21 April 2022, the controller explained to the complainant the consent given in the context of the raffle. The complainant also received a copy of the consent form.

II. Conclusion

At the end of its investigations, the CNPD concluded that the controller had sufficiently demonstrated the lawfulness of the contested processing under Articles 5 and 6 of the GDPR.
In view of the facts of the case and taking into account the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, the CNPD did not consider it necessary to pursue the complaint further.

It therefore contacted the BayLDA with the results of the investigations to date, which the BayLDA explained in its letter of 16 September 2022 to the complainant, asking whether, despite the findings to date, there were reasons for continuing the complaint in his view. BayLDA received no reply from the complainant and informed the CNPD thereof. The CNPD concluded that no further action was necessary and that the cross-border complaint could be rejected.

Consequently, the CNPD decided to reject the complaint and, via IMI, sent the relevant draft decision No. 538804 to the concerned supervisory authorities. The concerned supervisory authorities (including BayLDA) did not object to the draft decision.

In accordance with Article 60(8) of the GDPR, the final decision in the present case must be adopted by the BayLDA.

Ansbach, 17 August 2023

Our reference: LDA-1085.1-3798/20-F
IMI Art. 56: 166627
IMI draft decision: 521192

Controller: [redacted]

On the basis of the draft decision of the Dutch Autoriteit Persoonsgegevens (NL SA) No. 521192, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) pursuant to Article 60(8) of the GDPR issues the following

Final Decision:

The complaint is rejected.

Justification:

The complaint was received by the BayLDA on 18 April 2020 and was forwarded via IMI to the NL SA as the lead data protection supervisory authority for the controller.

On 30 May 2023 the NL SA submitted the draft decision no. 521192 to the concerned supervisory authorities with the following contents:

IMI Article 56 identification of LSA and CSA entry	166627
IMI Case Register entry	521146
National file number	LDA-1085.1-3798/20-F
Controller	Wallet Solutions
Date of receipt of complaint	18.04.2020

With regard to the abovementioned case and pursuant to Article 60(3) of the General Data Protection Regulation (GDPR), the Autoriteit Persoonsgegevens (Dutch Data Protection Authority, hereafter: NL SA) has issued the following draft decision:

Summary of the Case

1. On 30 November 2020 an article 56 notification with number 166627 was broadcasted by the Bavarian SA. As the controller at the time the complaint that was the subject of the article 56 procedure was established in the Netherlands, the NL SA considered itself the lead authority (LSA) in the matter, in accordance with article 56 GDPR.

2. The complainant had contacted controller – a debt collecting company - (in March and later again in May 2020) to request access to data and to be informed with regard to the origin of the data, processed by the controller, and whether the data had been transferred to any third party. The

complainant did not receive a satisfactory answer. That is why he filed a complaint with the Bavarian SA.

Investigation by the NL SA

3. Because of capacity, the complaint was not assigned to a case handler until 2022. Considering that quite some time had passed between the lodging of the complaint and the start of the active phase of case handling by the NL SA, the NL SA asked the complainant whether his complaint was still actual on 22 August 2022 (informally, per email) and on 22 October 2022 (officially, per VMAN over IMI – VMAN 446811).

4. The NL SA has not heard from the complainant, nor per email nor as the result of communications with the Bavarian SA over IMI.

Norm allegedly infringed

Articles 6, 12, 13, 14 and 15 GDPR.

Proposed action by the NL SA

1. Considering the lack of a response from the complainant to confirm whether or not the complaint has been resolved, the NL SA has no reason to believe that the processing of personal data was not lawful based on Articles 6, 12, 13, 14 and 15 of the GDPR.

2. Considering the above the NL SA finds no infringement of the GDPR in this case.

3. The NL SA deems this matter investigated to the extend appropriate and rejects the complaint ex article 60(8) GDPR. The supervisory authority with which the complaint was lodged (the regulatory authority in Bavaria) shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

As the concerned supervisory authorities (including BayLDA) did not object to this draft decision, the BayLDA hereby adopts this draft decision as final decision in accordance with Article 60(8) of the GDPR.

Ansbach, 17.08.2023

09.08.2023

Final decision

Complaint by [redacted] against [redacted] ([redacted]') of 29 June 2018 (IMI Notification No: 537956; Reference of the Bavarian State Office for Data Protection: LDA-1085.4-7273/18-I)

In the above matter, pursuant to Article 60(8) of the GDPR, the Bavarian State Office for Data Protection Supervision (BayLDA) adopts the following decision on the basis of the draft decision of the Luxembourg supervisory authority (National Commission for Data Protection Grand Duchy of Luxembourg (CNPD) of 13.7.2023):

Dismisses the complaint of 29 June 2018 by [redacted] against [redacted]

Reasoning:

I. Facts

After receiving [redacted]'s complaint to the BayLDA, it was prepared and forwarded to the lead supervisory authority, the CNPD, for transmission via IMI.

In his complaint, the complainant claimed that he had received multiple unsolicited products via [redacted]. He then contacted the company's customer service. From the correspondence with a customer service employee, the complainant has concluded that he has made contact with the consignor of the products and has disclosed to him/her personal data (e.g. name and address).

The main concern was that the competent data protection supervisory authority should investigate whether his personal data have been disclosed by an [redacted] employee and, and, if necessary, to take appropriate measures to prevent such business practices in future cases.

The CNPD concluded from this that the complaint is based on an infringement in the scope of Article 5(1)(f) GDPR.

In accordance with Article 57(1)(f) of the GDPR, the CNPD has contacted [redacted] and requested the company to comment on the facts described by the complainant, in particular to the processing of the complainant's personal data in the facts described in the complaint.

The company has complied with the request to send an statement, stating that the said orders were made by a customer account associated with a person bearing the same family name as the complainant (in the follow-up "third party" – note: both names are known to the CNPD and the BayLDA). In addition, the delivery address stored in this customer account is the same as the address of the complainant. Only two orders (on 13 and 14 May 2018) have been successfully placed through this account and it is clear from the records of the controller that Customer Service sent to this customer account on 13 and 14 May 2018 messages related to the orders, but no further communication took place in May or June 2018.

The controller had no evidence that an employee of the customer service exchanged personal data with the third party or that it was a case of so-called "brushing", given the common names and addresses and the limited number of products ordered in this way.

The CNPD has informed the controller that the complainant has provided an email from an employee of the controller dated 16 May 2018 informing the complainant that the employee has informed the third party of the complaint of the complainant and requested the third party to clarify the matter directly with the complainant. The complainant therefore had reason to believe that his personal data had been unlawfully passed on to the third party.

II. Legal assessment

The CNPD has determined that even taking into account the above e-mail, it is not possible to prove whether or which data the company's employee may have passed on to the "third party". It would be conceivable that the employee only described the journey to the third party without disclosing the identity of the complainant. In any case, it remains unclear (and not proven) which specific data may be affected (e.g. name and/or address). In addition, the employee concerned acted prudently by not disclosing the third party's personal data to the complainant, which in turn led the CNPD to assume that the controller's employees were aware of the importance that customer data should not be disclosed to other customers. The person responsible further confirmed that the said e-mail does not correspond to what is conveyed in the employee training courses.

The CNPD also noted that the complainant had filed a criminal complaint against unknown to the German law enforcement authorities, but was discontinued by the public prosecutor's office due to a lack of evidence.

Finally, it is apparent from the file procedure that the third party already knew the name and address of the complainant, since the third party had deposited the address in the customer account and had the parcels delivered to that address before communication with the company's employee had taken place.

As the lead supervisory authority, the CNPD has therefore decided that, following the conclusion of the investigation into the facts, there is no evidence that the controller has disclosed the complainant's personal data.

For the above reasons and taking into account the seriousness of the alleged breach of data protection law and the impairment of fundamental rights and freedoms in the area, the CNPD did not consider it necessary to pursue the complaint and reject it.

This decision was to be adopted by the BayLDA in accordance with Article 60(8) of the GDPR.

Bavarian State Office for Data Protection Supervision

Data Protection Authority of Bavaria
for the Private Sector

Data Protection Authority of Bavaria
for the Private Sector
Promenade 18 | 91522 Ansbach
Phone: 0981 180093 0
Fax: 0981 180093 800 postpost
E-mail: www.lda.bayern.de
Web:

29.08.2023

Final Decision for VMN 490333

Decision:

The Data Protection Authority of Bavaria for the Private Sector notes that [redacted] has infringed Article 12(3) of the GDPR by not reacting immediately to the complainant's request for deletion pursuant to Article 17 of the GDPR of 29.9.2022.

The Data Protection Authority of Bavaria for the Private Sector warns [redacted] in accordance with Article 58(2)(b) GDPR for breach of Article 12(3) of the GDPR.

Summary of the case:

As part of the cooperation between the European data protection supervisory authorities, the Data Protection Authority of Bavaria for the Private Sector has received the complaint of 2 November 2022, in accordance with the provisions of Article 60 of the GDPR, as the lead data protection supervisory authority (Article 56(1) of the GDPR), in which it was necessary to examine whether [redacted] infringed the right to erasure of the complainant.
The forwarding took place on 6.2.2023 by the Spanish data protection supervisory authority to which the complainant had lodged his complaint.

<u>Case of complaint:</u>
The complainant indicated that he had submitted a request for deletion to the controller on 29 September 2022. On 29.9.2022, the company's external data protection officer informed the complainant that his application had been forwarded to [redacted]. A further reaction of the data protection officer or the controller then no

longer took place.

<u> of the controller:</u>
The Data Protection Authority of Bavaria for the Private Sector requested a written opinion on the facts from the controller on 20 April 2023. This statement of the insolvency administrator of the company of 27.4.2023 states the following:
'...It is true that, by order of 30.1.2023, the Amtsgericht München appointed Mr. Attorney [redacted]. as insolvency administrator. We assume that the processing of Mr [redacted]'s personal data was based on an online order for the goods marketed by [redacted]. [redacted]'s business operations are now completely discontinued. We do not know whether the deletion request has reached [redacted] in the past. In any case, the data and information provided to us do not reveal any more information about a Mr. [redacted]....»

Statement of reasons for the decision:

In accordance with Article 17(1) of the GDPR, the data subject has the right to request the controller to delete personal data concerning him or her without undue delay, and the controller is obliged to delete the personal data without undue delay if one of the conditions set out in this Article is met, such as when the data is no longer necessary for the purposes for which they were collected or the consent to the processing is revoked by the data subject.
In accordance with Article 12(3) of the GDPR, the controller shall provide the data subject with information on the measures taken on request pursuant to Articles 15 to 22 without undue delay and in any event no later than one month after receipt of the request. This period may be extended by a further two months if necessary, taking into account the complexity and number of applications. The controller shall inform the data subject of an extension within one month of receipt of the request, together with the reasons for the delay.

The complainant's request for deletion pursuant to Art. 17 GDPR dated 29.9.2022 has been demonstrably received by the data protection officer of the controller. The corresponding confirmation of receipt is available. The exact date on which the complainant's personal data were deleted cannot be seen in the statement of 27.4.2023, obviously the insolvency administrator is not aware of this. However, the opinion confirms that the complainant's personal data could no longer be found, so it can be assumed that the erasure request has been implemented by the controller.
Regardless of the date of deletion, the controller failed to inform the complainant within one month of the measures taken on the basis of his request, i.e. about the execution of the deletion, to which he would have been obliged under Article 12(3) of the GDPR. This constitutes a violation of Article 12(3) of the GDPR.

Choice of supervisory measure:

It follows from Article 58(2)(i) and Article 83(2) GDPR that the data protection supervisory authorities are empowered to impose fines. According to the second sentence of recital 148, a warning may be issued in accordance with Article 58(2)(b) in the case of a minor infringement instead of a fine. The aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous, relevant infringements, must be taken into account.

Since the complainant's personal data has been deleted in the meantime and the Data Protection Authority of Bavaria for the Private Sector, as the lead data protection supervisory authority for this company, has not received any further complaints in connection with the data subject rights under the GDPR against this company in the past, the issuance of a warning pursuant to Article 58 (2) (b) of the GDPR is deemed sufficient in the present case.

Possibility of bringing proceedings:

With reference to Articles 77 and 78 of the GDPR, we would like to point out that this decision may be brought against:

Verwaltungsgericht Ansbach in 91522 Ansbach,
House address: Promenade 24 – 28, 91522 Ansbach
Postal address: PO Box 616, 91511 Ansbach

Information on the possibility of bringing proceedings:

The appeal may be lodged in writing, for minutes or electronically in a form authorised to substitute the written form. The filing of an appeal by simple e-mail is not allowed and has no legal effects!

Yours sincerely

[redacted]
Data Protection Authority of Bavaria for the Private Sector

—

Final decision

Complaint by Mr [redacted] against [redacted] ([redacted]') of 18 February 2020 (IMI Notification No: 5.914; Reference of the Bavarian State Office for Data Protection Supervision: LDA-1085.3-4347/20-I)

In the above matter, pursuant to Article 60(8) of the GDPR, the Bavarian State Office for Data Protection Supervision (BayLDA) adopts the following decision on the basis of the draft decision of the Luxembourg supervisory authority (National Commission for Data Protection Grand Duchy of Luxembourg (CNPD) of 13.7.2023):

The proceedings concerning Mr [redacted]'s complaint against [redacted] of 18.2.2020 29.06.2018 are closed.

Explanatory memorandum:

I. Facts

After Mr. [redacted]'s complaint was received by the Bavarian State Office for Data Protection Supervision (BayLDA), it was prepared for forwarding via IMI to the lead supervisory authority, the CNPD, and forwarded there.

In his complaint, the complainant argued that, during his absence, [redacted]'s delivery service had placed a package outside his door. However, this package was not addressed to him. In the case of a subsequent telephone call, the complainant was asked to indicate his date of birth. He did not do this because it was not his query. [redacted]'s employee then noticed that the complainant had a customer account with [redacted] and he knew when he was born. Upon asking the complainant how the employee knows this, the employee informed him of his phone number.

The main concern was that the competent data protection supervisory authority should investigate whether the data processing with regard to the complainant's personal data has been lawfully carried out (deposit and access to the date of birth) and, if necessary, to take appropriate measures to prevent such business practice in future cases.

The CNPD concluded that the complaint is based on infringements in the scope of Article 5(1)(a), Article 5(1)(b), Article 5(1)(f) of the GDPR.

In accordance with Article 57(1)(f) of the GDPR, the CNPD has contacted [redacted] and requested the company to comment on the facts described by the complainant, in particular to the processing of the complainant's personal data in the facts described in the complaint.

The Company complied with the request to send an opinion in due time, stating that there were no records of the interaction between the complainant and customer service, as a result of the limited retention period for customer service contacts. However, it may also be because the verification process was not completed and the contact was therefore not linked to the complainant's account. In any event, the conduct of the

customer service representative described by the complainant is not customary by default to identify customers who contact customer service by telephone. There were also no records of the date of birth of the complainant. The verification process does not include the date of birth of a customer.

In order to identify the misguided delivery and provide further information, it was necessary that the person responsible [redacted]) receives the order number specified on the package, as a delivery error could also be an explanation of the incident.

After consulting the complainant in this regard, the complainant said that the case could now be left to rest and that no further investigation should be carried out.

II. Legal assessment

After resolving the facts, the CNPD had to find out that without the order number on the package, the facts could no longer be clarified.

The CNPD, as the lead supervisory authority, in accordance with the complainant's statement to let the matter rest and not to investigate further, came to the conclusion that the complaint was considered withdrawn.

The procedure had to be closed.

This decision was to be adopted by the BayLDA in accordance with Article 60(8) of the GDPR.

The BayLDA asks the colleagues of the lead authority on their behalf to inform the controller of this decision.

Bavarian State Office for Data Protection Supervision
25.08.2023

Berlin Commissioner
for Data Protection
and Freedom of Information

521.11629
French DPA: 19003650
A56 ID 72416
CR 73122
DD 166113
IC 356451
DD 405144

1 September 2022

Final Decision

[redacted]

Dear Madam or Sir,

We hereby issue a reprimand to your company for a violation of the General Data Protection Regulation (GDPR).

Justification:

Our decision is based on the following considerations:

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Friedrichstr. 219, 10969 Berlin
Visitors' entrance: Puttkamerstr. 16-18

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

Office hours: Daily from 10 am to 3 pm, Thursdays from 10 am to 6 pm

Mail: mailbox@datenschutz-berlin.de
Web: www.datenschutz-berlin.de

BERLIN

I.
We have established the following facts:

The complainant submitted that when registering with the online game [redacted], he had provided an e-mail address containing his first and last name ([redacted]). On February 18, 2019, he wanted to change this e-mail address to a more anonymous e-mail address [redacted]. However, he was informed by customer support that this was (technically) not possible.

They informed the following in the above-mentioned letter:

The complainant with the e-mail [redacted] had wanted to try to transfer his player account to another player in 2017. However, this is not permitted under the terms and conditions of [redacted]

According to [redacted], no user is entitled to transfer or sell his user account to a third party or to allow a third party to use his user account without the prior consent of [redacted] consent to a transfer does not authorize the transfer of a user account for a fee or other consideration unless express permission to do so is given as part of the consent.

The background to this is to ensure that each player has achieved game progress on their own. Honest players should not be deterred in this way.

In 2017, the complainant had already once requested the correction of the e-mail address. At that time, he himself had admitted that it was the e-mail address of a friend. In his email of August 3, 2017, he had explained that the friend had already played the game, but had lost interest because of the poor internet connection. He further confirmed the request to correct the e-mail address to that of a friend in e-mails dated August 8 and 9, 2017.

Now the account should be changed to the e-mail address [redacted]. In your opinion, based on the incident in 2017, it could not be ruled out that it was again a matter of transferring the account.

In your opinion, this is not a matter of the right to rectification pursuant to Article 16 of the GDPR, as the e-mail [redacted] is still correct. No incorrect data would be stored. According to Article 16 sentence 2 of the GDPR, a data subject only has the right to request the completion of incomplete personal data - also by means of a supplementary declaration. In the case of the complainant, however, the old e-mail address was still valid. Accordingly, the old address was not an incorrect date. The complainant also did not demand that the new e-mail address be added to his data, but rather that it be exchanged with the old one and, to that extent, not supplemented. There was no reason to change the previous e-mail address to the new one for goodwill reasons.

In this case, the statement of technical reasons was made instead of a non-statement of reasons, which would also have been permissible from a legal point of view, or a reference to the general terms and conditions. According to you, this was done because there were indeed technical reasons, because it would create a considerable technical effort if a transfer of user accounts had to be permitted in the terms of use and then ensured (e.g., due to the necessary verification processes and necessary security measures for such a transfer).

In the opinion of [redacted], changing the e-mail address would also not lead to anonymization, as the name of the complainant was stored at [redacted] anyway due to the legal obligation to retain data. You also requested that it be noted that the complainant's e-mail address is only requested in your system during registration/login and does not appear anywhere else. In this respect, the complainant's argumentation regarding better anonymization did not apply. And the e-mail address you have in your system is always assigned to a specific user, who is also known by name from the time a contract is concluded - as in the case of the complainant. In this respect, too, there was no legitimate interest of the complainant in an alleged "anonymization" via an innocuous e-mail address.

Accordingly, changes to the e-mail address could only be made if it was ensured that the request for change was not based on a transfer of the account, i.e. the existing e-mail account verifiably no longer existed, for example.

Finally, the complainant had been notified of a supplementary (late) notice regarding his change request. However, this notice still does not refer to the prevention of the player transfer.

II.
Legally, we assess the facts as follows: Your company has violated the GDPR.

1. Violation of Article 12 (1-4) GDPR

According to Article 12 (3) of the GDPR, the controller must provide the data subject with information about the measures taken pursuant to Articles 15 to 22 of the GDPR within one month of receipt of the request. If he does not take any measures, he must inform the data subject of the reasons within the one-month period (Article 12 (4) GDPR).

Request for rectification pursuant to Article 16 GDPR.

The complainant's request constitutes a request for rectification of their data pursuant to Article 16 of the GDPR. Your argument that the previously stored e-mail address still works and is therefore not incorrect is not valid. In principle, every person is free to decide for themselves which e-mail address they would like to use for which communication purpose.
In particular, every person must be free to gradually deactivate or withdraw a particular e-mail address from circulation in order to be able to switch it off at some point, e.g. because the provider is to be changed or because too many unwanted e-mails reach them at a particular e-mail address.

Accordingly, the accuracy of an e-mail address not only requires that it can be objectively assigned to the data subject, but also requires that the specific e-mail address has been designated by the data subject for the specific communication purpose. The data subject can also change this designation. With the e-mail of February 18, 2019, the complainant informed you that he would like to use a different e-mail address for communicating with you in the future. He thus changed the purpose for his e-mail address previously stored with you; it was no longer intended for communication with you. It was therefore incorrect.

The request pursuant to Article 16 of the GDPR had to be answered in accordance with Article 12 (3), (4) of the GDPR.

No sufficient communication pursuant to the first sentence of Article 12 (1) GDPR.

Communications pursuant to Articles 12 to 22, i.e. also pursuant to Article 16 GDPR, must be provided in a precise, transparent, comprehensible and easily accessible form in clear and simple language pursuant to the first sentence of Article 12 (1), GDPR. This also means that the data subject is informed transparently about the real background of the refusal of the rectification according to Article 16 GDPR.

In the present case, the true reason for the refusal was not communicated to the complainant, but only relied on technical reasons. In the French reply of the support of February 19, 2020, it was stated that the necessary architecture to change this information had not been available.

In addition, it was explained that a rectification pursuant to Article 16 of the GDPR could not be considered, as the e-mail address could not be incorrect since it was still functioning. However, this alone does not exclude the right to rectification under Article 16 GDPR (see above).

The reason given to us that there are doubts as to whether the newly provided e-mail address is actually an address of the complainant and that there are fears that the account could be passed on in breach of contract was not transparently informed to the complainant. This is a violation of Article 12 (3) in conjunction with (1) of the GDPR.

2. Right to rectification in the specific case

The right to rectification exists, of course, only if the processed data do not become inaccurate as a result of the change requested by the complainant. The controller is responsible for this in accordance with Article 5 (1) (d) GDPR. Insofar as there are reasonable doubts that the new e-mail address provided by the complainant is one of the complainant, your company may take appropriate measures to ensure the accuracy of the information. However, it must always be taken into account that the company must facilitate the exercise of the right of rectification under Article 16 of the GDPR in accordance with Article 12(2) of the GDPR.

III.
As a result, we have decided not to take any further supervisory measures due to the violation, but to leave it at a reprimand for the time being.

The reprimand is based on Article 58 (2) (b) of the GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after the conclusion of our investigation. When approached by us, you showed understanding and announced that you would comply with data protection requirements and cease the reprimanded behavior.

In the certain expectation that you will comply with data protection regulations in the future, we consider the matter closed.

[Information on legal remedies not translated]

Berlin Commissioner
for Data Protection
and Freedom of Information

521.13177.27
IMI CR 175641
A60DD 431495

November 4, 2022

Final Decision

[redacted]

Reprimand
Complainant: [Redacted]
Your letters of 15 December 2020 and 29 April 2021

Dear Mr. [Redacted],
The Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA) hereby reprimands your company for an infringement of the General Data Protection Regulation (GDPR).

Reasoning:

The Berlin DPA bases this decision on the following considerations:

I.
The Berlin DPA has established the following facts:

The complainant submitted that he placed an order with [redacted] on 16 June 2020 with the number [redacted]. Subsequently, [redacted] passed on hisdata to [redacted]. The complainant had then received a delivery notification from them by e-mail. The

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Alt-Moabit 59-61, 10555 Berlin
Germany

Phone: +49 30 13889-0
Fax: +49 30 215 50 50
Office hours: Monday to Friday from 10 am to 3 pm, Thursday from 10 am to 6 pm

E-mail: mailbox@datenschutz-berlin.de
Website: www.datenschutz-berlin.de

BERLIN

complainant stated he had not given his consent to the forwarding of your data to [redacted]

[redacted] informed us that the complainant had consented to the transfer of his data to [redacted] by confirming the General Terms and Conditions of Business (GTC) and the data protection declaration as part of the order. [redacted]

Furthermore, [redacted] submitted that it employs less than nine employees who are entrusted with the processing of personal data. The managing director of [redacted] is also the data protection officer.

II.

Legally, the Berlin DPA assesses the established facts as follows:

The company has infringed the GDPR.

1. Infringement of Art. 5 (1) and Art. (6) (1) GDPR

Your company has violated Art. 5 (1) and Art. (6) (1) GDPR, as the transfer of the complainant'se-mail address to [redacted] took place without a legal basis.

The permissibility of data processing follows the principle of prohibition with reservation of permission. Accordingly, any data processing must comply with the principles set forth in Art. 5 (1) GDPR as well as at least one of the legal bases set forth in Art. 6 (1) (a) to (f) GDPR. In the present case, a legal basis for the data processing is not apparent.

a) There is no effective consent within the meaning of the first sentence of Art. 6 (1) (a) GDPR.

[redacted] has submitted that the complainant has confirmed to have read the GTC. The GTC in turn contained the data protection declaration with a reference to the transfer of data to the respective parcel service provider. From this, [redacted] deduces the consent to the data transfer. Irrespective of the question of whether effective consent can be given in this way at all, the Berlin DPA does not have sufficient proof of consent to the GTC within the meaning of Art. 7 (1) GDPR.

Furthermore, such a confirmation that the GTC have been read is invalid pursuant to Section 309 No. 12 b) German Civil Code. According to Section 309 No. 12 b) German Civil Code, a provision by which the user changes the burden of proof to the detriment of the other party to the contract, in particular by having the other party to the contract confirm certain facts, is invalid. If a pre-formulated read confirmation is obtained by clicking on a checkbox, this involves an inadmissible reversal of the burden of proof to the detriment of the customer, which results in the invalidity.

Moreover, an effective consent to data processing can only be obtained through the use of general terms and conditions in exceptional cases. According to Art. 4 (11) GDPR, consent is 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.

In the event that the data subject's consent is given by means of a written statement, which also concerns other matters, Art. 7 (2) GDPR provides that the request for consent must be made in an intelligible and easily accessible form in plain and simple language in such a way that it can be clearly distinguished from the other matters. This rule also applies to electronic declarations. Therefore, the consent would have to be clearly emphasised in the GTCs, for example by placing it in bold, framing it or highlighting it in colour (emphasis requirement). It must also be clearly indicated in the text requesting consent to the GTC that consent under data protection law is also obtained with the confirmation and for what purpose. This is to ensure that the data subject makes the declaration of consent consciously and in an informed manner and that this is not lost in the context of the confirmation of the GTC.

Also, the wording in the GTC of [redacted]

[redacted] is only of an informative nature and is therefore not suitable for obtaining an effective consent. It is not clear from the wording that consent to the data transfer is to be given by confirming the GTC. Furthermore, the text part is not visually distinguishable from the rest of the text.

Additionally, the voluntary granting of consent requires that the data subject has a genuine choice. Pursuant to Art. 7 (4) GDPR, it must be ensured that the performance of a contract or the provision of a service is not made dependent on consent to data processing that is not necessary for the performance of the contract. In the present case, the transmission of the e-mail address to [redacted] is not necessary for the performance of the contract, as the delivery information could be passed on to the customer by the company itself, for example by means of a link to track the shipment. In addition, it is assumed that consent was not given voluntarily if - as in the present case - consent is a non-negotiable part of the terms and conditions (cf. European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, p. 8).

The first sentence of Art. (1) (a) GDPR can hence not serve as a legal basis.

b) Other legal bases, the first sentence of Art. 6 (1) (b) to (f) GDPR

The transmission of the e-mail address to [redacted] cannot be based on a legal basis of the first sentence of Art. 6 (1) (b) to (f) GDPR. In this respect, only the first sentence of Art. 6 (1) (b) and (f) GDPR come into consideration. In both cases, however, the necessity of the data processing is lacking.

2. Infringement of the second sentence of Art. 38 (6) GDPR

There is an infringement of the second sentence of Art. 38 (6) GDPR. According to the second sentence of Art. 38 (6) GDPR, the controller or processor must ensure that other tasks and duties of the data protection officer do not lead to a conflict of interest.

Due to this rule, the office of the data protection officer cannot be held by a key decision-maker of a company, such as a member of the controller's management. According to the first

sentence of Art. 38 (6) GDPR, a data protection officer may take on other tasks and duties, but these may not lead to a conflict of interest. The data protection officer shall exercise his/her duties and tasks in complete independence (cf. recital 97). It is not compatible with the position and function of a data protection officer if he or she would have to control his or her own activities. Such an overlap of the spheres of interest would impair the required complete independence of the data protection officer. Since the function of the data protection officer in the present case is exercised by the managing director, there is an infringement of the second sentence of Art. 38 (6) GDPR. In this respect, it is irrelevant if the managing director himself is of the opinion that there is no conflict of interest and that the required independence exists.

An infringement must also be established if, pursuant to Art. 37 (1) GDPR, possibly in conjunction with Section 38 (1) German Federal Data Protection Law (BDSG), there is no obligation to appoint a data protection officer, but such an officer is appointed voluntarily (first sentence of Art. 37 (4) GDPR). The existence of an obligation to appoint a data protection officer is not evident in the case of [redacted]. In particular, the threshold of the first sentence of Section 38 (1) BDSG, according to which a data protection officer must be appointed if a controller generally employs at least 20 persons on a permanent basis with the automated processing of personal data, has not been met. However, the company has voluntarily decided to appoint a data protection officer. If a company voluntarily decides to appoint a data protection officer, this leads to a full application of Art. 37 to 39 GDPR (Art. 29 Working Party on Data Protection, Guidelines on Data Protection Officers ("DPO"), WP 243 rev.01, p. 6).

III.

As a result, the Berlin DPA does not intend to take any further supervisory measures due to the infringement, but to leave it at a reprimand.

The reprimand is based on Art. 58 (2) (b) GDPR.

With regard to the infringement under 1. (Art. 5 (1), 6 (1) GDPR), this is already your second infringement, so the Berlin DPA assumes that [redacted] acted in full knowledge of the

facts. Nevertheless, the Berlin DPA decided to leave it at a reprimand once again, taking into account the circumstances [redacted] has presented:

[redacted] has stated that after the first infringement was discovered by the Berlin DPA, [redacted] commissioned a service provider with the logistics of [redacted] online trade, as a result of which the transmission of the e-mail addresses to the parcel service providers was stopped. However, due to pandemic losses in turnover, [redacted] could not continue to employ the service provider, so that [redacted] initially reverted to the previous solution in order to maintain its business. In the meantime, however, [redacted] had changed its practice again so that e-mail addresses were no longer transmitted to the parcel service providers. Due to the fact that the violation was stopped immediately, in which the procedure was changed again and as it was an individual case, we have decided to issue a reprimand here.

The Berlin DPA has taken into account the fact that [redacted] has been reasonable and has already stopped the behaviour complained of in relation to infringement 1. The Berlin DPA has also taken into account that the company is a small to medium-sized enterprise. Even though small and medium-sized companies are equally bound by data protection regulations, they are generally not able to provide comparable resources as larger companies for checking compliance with data protection regulations and making any necessary adjustments. However, the Berlin DPA would like to point out that it reserves the right to re-examine compliance with data protection regulations.

With regard to infringement 2 (Second sentence of Art. 38 (6) GDPR), [redacted] announced that it would review the appointment of an external data protection officer. The Berlin DPA assumes that [redacted] will immediately remedy the alleged infringement on its own.

In the certain expectation that [redacted] will comply with the data protection regulations in the future, the Berlin DPA considers the matter closed.

[Legal Notice not translated]

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

632.257.1
521.12260
Austrian DPA D130.354
CR 52519
DD 174148
FD 191920

OUTFITTERY GmbH
Management Board
Ms. [redacted]
Leuschnerdamm 31
10999 Berlin

16 March 2021

Reprimand
Complainant: Mr. [redacted]
Your letters of 16. March 2020, 22. June 2020 and 9. October 2020 (your ref. IS-0472-10)

Dear Ms. [redacted],

The Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA) hereby issues a reprimand to your company for a violation of the General Data Protection Regulation (GDPR).

The Berlin DPA bases the reprimand on the following considerations:

I.
The Berlin DPA has established the following facts:

The complainant had received a confirmation via email regarding the erasure of his personal data by the controller Outfittery GmbH on 12 April 2019.

According to the commercial register (Charlottenburg Court, HRB 140519 B), the Curated Shopping GmbH, with its registered office in Berlin (Charlottenburg Court, HRB 138459 B), is merged with the Outfittery GmbH as a whole on the basis of the merger agreement of 17 June 2019 and the consent resolutions of the same date by transferring its assets with dissolution without liquidation as of the merger date of 27 June 2019 (date of entry in the commercial register). Pursuant to § 2(1) of the aforementioned merger agreement, Curated Shopping GmbH has transferred its assets as a whole with all rights and obligations to Outfittery GmbH under dissolution without liquidation pursuant to § 2(1) of the Transformation Act (merger by absorption).

On 24 July 2019, the complainant had also requested erasure of his personal data to the controller Curated Shopping GmbH, which is the provider

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.

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/beschwerde.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

be Berlin

of the service MODOMOTO, by contacting the address team@modomoto.at, and had received a confirmation of his request from this address via email.

On 19 October 2019, the controller informed the complainant by email about the transfer of his data into the Outfittery GmbH system and the creation of his new account with Outfittery GmbH and requested him to activate his account. The complainant again requested the controller to erase his personal data by email on 21 October 2019.

By credible comments dated 16 March 2020, the controller admitted that he had not implemented the complainant's erasure request of 24 July 2019 due to an error on the part of an employee and had only erased the complainant’s personal data on 24 January 2020. In further comments of 22 June 2020, the controller also admitted that he had not sent a deletion confirmation to the complainant.

II.
In legal terms, the Berlin DPA assesses the facts of the case as follows. The controller has violated the General Data Protection Regulation.

According to Article 5(1)(a) GDPR, personal data must be processed in a lawful manner. In order for the processing to be lawful, personal data must be processed either with the effective consent of the data subject or on the basis of a legal authorisation, according to the first sentence of Article 6(1) GDPR.

Through his erasure request of 24 July 2019 pursuant to Article 17(1) GDPR, the complainant expressed that he was not interested in continuing the customer relationship with Curated Shopping GmbH, which at that time had already merged with Outfittery GmbH. Further processing of his data for the business purposes of Outfittery GmbH was thus no longer necessary.

However, the complainant’s request for erasure was not implemented due to an internal employee error at Outfittery GmbH. Instead, the complainant's data was reused on 21 October 2019 by creating an account in Outfittery GmbH's systems and informing the complainant accordingly, although the complainant's data should have been erased based on his previous request for erasure.

The fact that the implementation of the complainant's deletion request of 24 July 2019 was not implemented by Outfittery GmbH due to an internal employee error is irrelevant in this respect, since pursuant to Article 24(1) GDPR, Outfittery GmbH must ensure compliance with its obligations under data protection law by taking appropriate technical and organisational measures. In any case, Outfittery GmbH could also be expected to ensure that the content of the complainant's request for erasure was processed correctly by taking internal organisational measures.

The use of the complainant's data and its continued storage until erasure on 24 January 2020 thus took place without legal basis.

In addition, according to the first sentence of Article 12(3) GDPR, the controller must provide the data subject with information on the measures taken upon request pursuant to Articles 15 to 22 GDPR without undue delay, and in any case within one month of receipt of the request. This means

that the controller confirms the erasure or at least informs why this is not possible within the time limit. This deadline may exceptionally be extended by a further two months if this is necessary, taking into account the complexity and number of requests. However, a routine and blanket extension of the deadline without examining the individual case is not provided for by the GDPR. The controller also did not inform the complainant about an extension of the deadline and the reasons for it.

Consequently, the implementation of the complainant's erasure request of 24 July 2019 on 24 January 2020 was late. Moreover, the complainant was not informed about the erasure of his data by Outfittery GmbH, as the aforementioned acknowledgement of receipt of 29 July 2010 does not contain such information.

Consequently, Outfittery GmbH also committed a violation of Article 12(3) GDPR.

Outfittery GmbH has thus violated Article 5(1)(a), Article 6(1), Article 12(3), Article 17(1) and Article 24(1) GDPR.

III.
As a result, the Berlin DPA does not to take any further supervisory measures as a result of the infringement, but to leave it at a reprimand.

The reprimand is based on Art. 58(2)(b) GDPR.

Taking into account the specific circumstances of the case under investigation, the Berlin DPA considers a reprimand to be appropriate after completion of the investigation. The Berlin DPA has therefore established another violation on the controller‘s part.

In the safe expectation that the controller will comply with the data protection regulations in the future, the Berlin DPA closes this case after issuing the reprimand.

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

535.2128
631.326
CR 187764
DD 187943
FD 291424

Berlin, 23 April 2021

Final Decision

1. Core information on the data breach

Controller	Sandbox Interactive GmbH
Incident	In the forum of Albion Online (https://forum.albi-ononline.com), a security gap was exploited. The security gap had its origin in a forum software provided by a third party (WoltLab Burning Board). The controller was using the most current version of the software.
Time of the incident	unknown, probably also 16 October 2020
Time when the incident was known	16 October 2020, 22:51 Extortion email received
Affected EU/EEA member states	~ 293.000 affected in total. Since users only provide an email address to register and due to the high number of affected individuals, it must be assumed that all EU countries are affected.
Category of affected data subjects	Online gamers
Category of data types/records affected	Email addresses and password hash values (bcrypt)
Likely consequences of personal data breach:	Email addresses could be used to send promotional or malicious code emails

2. Description of the data breach from the technical-organizational point of view

In the forum of Albion Online (https://forum.albiononline.com), the security gap described below was exploited in a forum software of the third-party provider WoltLab Burning Board. The controller had made sure to have the latest version. The attacker/hacker tried to blackmail the provider.

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.

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/beschwerde.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

be Berlin

The exploited security gap was a flaw in the image upload function of the software. The third-party provider's software did not effectively prevent an attacker from using the image upload function to upload code and then execute it by exploiting the security gap in the third-party software.

In this regard, the company´s layers state: "The attacker apparently managed to manipulate an image file so that he could hide an exploit kit called C99 Shell in it. The security gap in the forum software was based on the fact that files uploaded by users could be executed under certain circumstances. Our client's customizations closed this attack path. The subsequent penetration test was unable to exploit this (and possible other) vulnerabilities. It is thus clear that the current configuration of the software used is secure."

Security gaps such as buffer overflows are widespread and occur regularly even in well-maintained standard software. Once detected, these vulnerabilities are usually fixed more or less quickly by new versions or patches of the respective software.

An analysis of the attack using the available log files showed that the attacker had tried unsuccessfully to work his way into other systems. The corresponding protective measures were effective.

In this regard, the company´s lawyers state: "Our client immediately isolated the entire infected server and took it offline as soon as they became aware of the incident. Our client stored the server for investigation and prosecution purposes in the same condition as the attacker left it. Our client reverse-engineered the attack script and determined that it was a multi-encoded (via base64 encode and php eval) exploit kit called C99 Shell. The exploit kit was used by the attacker to install the Adminer database frontend, which was then used to download backups of the forum database. However, the attacker's attempts to penetrate even deeper into the systems and onto other servers of our client were prevented by further security measures already in place at the time (including IP restrictions)."

This is the first data breach report from this particular controller.

3. Description and analysis of the effectiveness of the measures taken to address the data breach or mitigate any negative consequences (Article 33 (3) (d) GDPR).

The security gap was found by analyzing the attacker's activities on the systems and closed immediately. The affected server was taken offline and new internal system passwords were assigned.

On 17 October 2020 at 14:40 o'clock the forum was restarted on a new server. The affected users were asked to change their passwords. In addition, the login had already been secured with a second factor since December 2015: When attempting to log in from a previously unused device, a code from a confirmation e-mail needs to be entered.

With the closure of the specific security gap, several penetration tests and the upcoming switch of the forum software to another provider (which is the medium-term plan) it is ruled out that the security gap can still be exploited.

4. Notification of the affected parties or public announcement (Article 34 (1) or Article 34 (3) (c) GDPR)

Data subjects were notified by e-mail on 17 October 2020. In addition, information about the attack was posted on the forum page. Users were also advised to change their passwords for other services if the same password was used there.

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

HTTPS encryption and two-factor authentication were already in place. The passwords were hashed (bcrypt).

6. Subsequent measures by which the controller has ensured that a high risk to data subjects is unlikely to persist (Art. 34 (3) (b) GDPR).

See Section 3.

7. Measures intended by the Lead Supervisory Authority (Berlin DPA)

The Berlin DPA intends to discontinue the procedure, since the data subjects were informed comprehensively and quickly and this was the first data breach notification by the controller. No negligence can be attributed to him, since the security vulnerability occurred in a third-party software in the latest version, and sufficient technical and organizational measures were taken after the security gap was discovered. It must be taken into account that a large number of data subjects are affected. However, given that only the e-mail addresses were affected, only few and no special categories of personal data are affected per data record.

The Berlin DPA

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin DPA: 521.1255 / 631.186.3
Austrian DPA: D155.023

Novum Import GmbH
Address unknown

Berlin, 1 October 2021

FINAL DECISION

In line with Article 60(8) GDPR the Berlin DPA adopts the following Final Decision that has previously been submitted by the LSA, the Austrian DPA, as Draft Decision. This Final Decision has been slightly edited for clarity.

R U L I N G

The Data Protection Authority decides on the data protection complaint of [redacted] (complainant) dated 12. December 2019 against Novum Import GmbH (opponent) for violation of the right to deletion as follows:

- The complaint is dismissed.

Legal basis: Articles 51(1), 57(1)(f) and 77(1) of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter: GDPR).

R E A S O N S

A. Claims of the parties and proceeding

1. The complainant alleged in his complaint of 12. December 2019 with the Berlin Commissioner for Data Protection and Freedom of Information, which initiated the proceedings, that the opponent had violated his right to erasure, as well as by unlawful processing, by not responding to his multiple requests to delete his e-mail addresses from the advertising mailing list. The complainant received advertisements from the opponent several times a day without having registered his two e-mail addresses [email 1] and [email 2] for this purpose. The same advertising with changed sender address for toe spreaders had already been sent to the complainant about 100 times. It was not possible to unsubscribe, neither could the complainant unsubscribe himself directly through a link (unsubscribe link) on the newsletter, nor did the opponent, which had been contacted via a contact form on the website <http://zehen-abstandhalter-de, complied with the multiple requests for deletion. In the legal notice, the opponent was indicate with its registered office in Vienna and the tax number: 24728164-2-42. The complainant is almost not able to use his own webshop anymore, as he needs the two e-mail addresses for this purpose.

The complainant stated on 7 February 2020 that he received six to twelve advertising e-mails per day from the opponent under the subject "Team for

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.

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

be Berlin

Health Tips". In addition, further e-mails for other products (solarlights, drain cleaners, mouth-nose protection masks) have been sent.

In his statement of 23. April 2020, the complainant stated that he continues to receive advertising e-mails from different websites (www.solar-lampe-mit-bewegungsmelder.com, http://professioneller-messerschleifer1-de.com/index.php?page=contact and https://masken-infos-de.com/media/tac.php), all operated by the opponent. Despite multiple clicks on the “Unsubscribe link”, advertising messages were still sent by e-mail.

The complaint attached a set of screenshots of the website, footage of the received advertising, as well as the request for deletion by the contact form on the opponent’s homepage as well as a copy of the police report against the opponent.

2. The Berlin Commissioner for Data Protection and Freedom of Information uploaded the case in the "Internal Market Information (IMI) System", which is used in the context of the consistency mechanism to handle cross-border procedures under the provisions of GDPR. The imprint of the opponent indicated, that the headquarters are in Vienna.

3. The Austrian Data Protection Authority has not been able to send the request to the opponent because the address of Novum Import GmbH is unknown and a Company Registry consultation was also negative. This means that in the course of the check of the Company Registry on 30. June 2021, no company under this name is or was registered in the Company Register. Likewise, the query of <[redacted]> on June 30, 2021 did not lead to any search results. In addition to these data given in the imprint, the specified tax number <24728164-2-42> is also incorrect. Such a number is not awarded in Austria. Also, a “Whois” domain query has been carried out by the website addresses <http://zehen-abstandhalter-de> and <http://www.v9-laser-detector-de.com/index.php?page=rules>. The website <http://zehen-abstandhalter-de> is not active anymore.

The documented investigation steps of the Data Protection Authority are as follows:

Checking the website <http://zehen-abstandhalter-de>:

504 DNS look up failed

Die Webseite existiert nicht. Bitte überprüfen Sie die eingegebene URL. Klicken sie auf zurück um auf die vorige Seite zurückzukehren.

URL: http://zehen-abstandhalter.de/

Client IP: 10.4.161.38
Server IP: N/A
User name:
Group name:

Imprint from the page < http://www.v9-laser-detector-de.com/index.php?page=rules>:

Entwickler und Betreiber dieses Online-Webshops (im Folgenden: Webshop) ist:

NOVUM IMPORT GMBH – Herr [redacted]
WIEN - AUSTRIA
Steuernummer: 24728164-2-42

Kontakt

Company Registry query of < Novum Import GmbH>:

Suchbegriff
eingetragene und gelöschte Firmen (keine Zweigniederlassungen) eingeschränkt auf
Firmenwortlaut: Novum Import Gmbh

Suchergebnis
Zu den oben angeführten Suchbegriffen wurde kein Ergebnis gefunden.

erstellt vom Bundesministerium für Justiz ********** HA031B
für den Amtsgebrauch ********** 30.06.2021 14:02:06,019 26619859 ** ZEILEN: 0

Company Registry person query of < [redacted]>:

Suchbegriff
natürliche Person eingeschränkt auf
Zuname: [redacted]
Vorname: [redacted]

Suchergebnis
Zu den oben angeführten Suchbegriffen wurde kein Ergebnis gefunden.

erstellt vom Bundesministerium für Justiz ********** HA035
für den Amtsgebrauch ********** 30.06.2021 14:00:48,181 02302183 ** ZEILEN: 0

Whois query <http://www.v9-laser-detector-de.com>:

Whois Ergebnisse zu Ihrer Domain

Aktueller Besitzer
Domain Administrator
See PrivacyGuardian.org
1928 E. Highland Ave. Ste F104 PMB# 255
Phoenix
AZ

B. Subject of appeal

The object of the appeal is whether the complainant has been infringed in his right to deletion.

C. Findings of facts

The Austrian Data Protection Authority shall base its decision on the facts set out in point A and documented in the files.

The opponent's name, as well as the imprint, could not be assigned to any natural or legal person.

Assessment of evidence: The findings are based on the complaint initiating the proceedings of 12 December 2019, as well as the complainant's supplements dated 7 February 2020 and 23 April 2020 and the official research dated 30 June 2021 (Company Registry, query of persons in the Company Registry, Whois query).

D. From a legal point of view, it follows:

In accordance with Article 77(1) GDPR, without prejudice to any other administrative or judicial remedy, each 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 concerning him or her infringes this Regulation.

In accordance with Article 57(1)(f) GDPR, the supervisory authority must deal with a complaint and examine the subject-matter of the complaint to an appropriate extent. In Recital 141 in the second sentence, it is stated in more detail that the investigation following an appeal should go as far as is appropriate in individual cases.

The opponent could be identified by the complainant by the information contained in the imprint of the website (name). Despite a search in the Company Registry, a person query in the Company Registry and a Whois query, the controller could not be determined.

Although all conceivable investigations have been carried out, however, it has not been possible to locate the opponent. A further investigation of the complaint is not possible. The Data Protection Authority has fulfilled its obligation under Article 57(1)(f) GDPR and investigated the complaint to the appropriate extent.

It was to be decided according to the ruling.

Berlin Commissioner
for Data Protection
and Freedom of Information

521.13974 / 631.342

CR: 290757

IMI DD 344664

Berlin, 05 May 2022

Final Decision

Preliminary remarks

The complaint (ref. no. 521.13974 / 631.342) was raised before the Berlin DPA in January 2021. It was transferred to the supervisory authority Netherlands, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by Uber B. V., in accordance with Article 56 GDPR. The LSA Netherlands conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. The LSA Netherlands proposed a Draft Decision and thereby the complaint was rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

> With regard to the abovementioned case and pursuant to Article 60(3) of the General Data Protection Regulation (GDPR), the Autoriteit Persoonsgegevens (Dutch Data Protection Authority, hereafter: NL SA) has issued the following draft decision:
>
> **Summary of the Case**

On 15 March 2021 an article 56 notification with number 184404 was broadcast by the Berlin SA. On 24 March 2021 the NL SA indicated that we considered ourselves the lead authority in this matter, in accordance with Article 56 GDPR. On 20 April 2021 the Berlin SA broadcast an article 61 Voluntary Mutual Assistance Notification with number 290775 using Case Register Entry 290757.
The complainant wrote that he received a newsletter from Uber and that in the email he could not find an option to simply unsubscribe. He tried to unsubscribe by replying to the sender's address (uber@uber.com), but the e-mail bounced. He then sent a complaint to his local data protection authority.

Norm allegedly infringed

- Article 12 (2) GDPR states that the controller shall facilitate the exercise of data subject rights under Articles 15 to 22 GDPR.
- Article 21 (2) GDPR states that 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, which includes profiling to the extent that it is related to such direct marketing.

The complainant states that he could not unsubscribe from the marketing emails that Uber was sending him by using the reply function.

Investigation by the NL SA

On 15 October 2021 the NL SA sent an inquiry to Uber regarding this case. Uber replied on 1 November 2021 that Uber carried out internal research and has come to the conclusion that at the bottom the relevant email contains a link with the title: "Email settings", or in German: "E-Mail-Einstellungen". This link refers to a web page of Uber where users can unsubscribe (and, if desired, resubscribe) for different types of communication. The user has not made use of this link.
Uber wrote to the NL SA that since the date of the complaint the link has been modified in order to be more clear to the user. It now bears the title: "Email abbestellen" (unsubscribe). Uber added that the data subject has now been unsubscribed from marketing emails after the NL SA contacted them.

Furthering the statements of Uber the NL SA has checked the e-mail that the data subject complaint about and the NL SA established that it does indeed contain a link called "E-Mail-Einstellungen".
The NL SA has also reviewed the privacy policy on the website of Uber (https://www.uber.com/legal/nl/document/?name=privacy-notice&country=germany&lang=de) and established that it clearly describes the steps data subjects should take to unsubscribe from marketing emails.
The NL SA holds that the GDPR does not prescribe that unsubscribing should always be possible using the reply function. Furthermore NL SA established that the controller did offer an unsubscribe option with the link "E-Mail-Einstellungen" included at the bottom of the e-mail. Also Uber agreed to clarify to the name of the button. It now reads "Unsubscribe". Uber facilitates right of data subjects to object as required per Article 12(2) jo. article 21 GDPR. By actually unsubscribing the complainant from marketing emails it has facilitated the right to object of the complainant.

Proposed action by the NL SA
Thus, based on the above-mentioned explanations, the NL SA did not identify any infringement of the obligations set out in articles 12(2) and 21 Regulation (EU) 2016/679 (GDPR) by the controller. The NL SA has rejected the complaint according to Article 60 (8) GDPR. Henceforth, the cross border complaint case (national reference 521.13974 / 631.342) should be closed.

Appeal Notice to the complainant

Against this decision a lawsuit before the Verwaltungsgericht Berlin (administrative court of Berlin), Kirchstraße 7, 10557 Berlin is admissible. The lawsuit needs to be filed in written form within one month after the notification of this decision, it can also be filed as an electronic document with a qualified electronic signature (QES) or for the record of the clerk of the court. Please, note that in case of filing the lawsuit in writing the legal deadline is only met if the lawsuit reaches the administrative court within the deadline.

The Berlin Commissioner for Data Protection and Freedom of Information

Berlin Commissioner
for Data Protection
and Freedom of Information

521.14730 / 631.410
CR: 134712
Draft Decision IMI A60DD 372925

Berlin, 26 April 2022

Final Decision

Preliminary remarks

The complaint (ref. no. 521.14730 / 631.410) was raised before the Berlin DPA in July 2021. It was transferred to the supervisory authority Sweden, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by Klarna Bank AB, in accordance with Article 56 GDPR. The LSA Sweden conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. The LSA Sweden proposed the Draft Decision 372925 and thereby the complaint was dismissed /rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

> **“ Decision of the Swedish Authority for Privacy Protection (IMY)**
> The Authority for Privacy Protection (IMY) finds that Klarna not has processed personal data in breach of Articles 12.3, 12.6 and 15 of the General Data Protection Regulation (GDPR) 1 .
>
> The case is hereby closed.

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Friedrichstr. 219, 10969 Berlin
Visitors‘ entrance: Puttkamerstr. 16-18

Phone: (030) 13889-0
Fax: (030) 215 50 50
Office hours: Daily from 10 am to 3 pm, Thursdays from 10 am to 6 pm

Mail: mailbox@datenschutz-berlin.de
Web: www.datenschutz-berlin.de

BERLIN

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has 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 complainant has lodged their complaint (Germany, Berlin) 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 a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in the Czech Republic, Denmark, Germany, Finland, Norway and Poland.

The complaint

The complaint states the following. On 6 June 2021, the complainant requested access to his personal data pursuant to Article 15 of the GDPR. When Klarna did not reply, a reminder of the request for access was sent on 11 June 2021 and 17 June 2021.

What Klarna has stated

Klarna is the data controller for the processing to which the complaint relates. The request was received by Klarna on 6 June 2021. Klarna has dealt with the request received and has taken the following steps. On 11 June 2021, Klarna's customer service requested the complainant to complete their request with information regarding the complainant's identity and requested the complainant's telephone number in order to send a verification code(to access the personal data). The complainant then provided the information regarding identity without giving a telephone number. On 17 June 2021, the complainant requested that the request be dealt with by 19 June 2021.

On 24 June 2021, Klarna's customer service again asked the complainant to provide a telephone number. The complainant submitted the information on the same day. The register extract with password was sent to the complainant on 12 July 2021. Klarna considers

that the extract of the register has been submitted within the timeframe set out in Article 12(3) of the GDPR after the complainant has provided the necessary information regarding their identity.

Justification of the decision

Applicable provisions, etc.

Article 12(3) of the GDPR requires the controller to provide the data subject, upon request, without undue delay and in any event no later than one month after receiving the request, with information on the actions taken pursuant to, inter alia, Article 15. The one-month time limit may be extended by a further two months where the request is particularly complex or the number of requests received is high. If the time limit of one month is extended, the controller shall inform the data subject of the extension. Notification of the extension of the deadline shall take place within one month of receipt of the request. The controller shall also indicate the reasons for the delay.

Without prejudice to Article 11, where the controller has reasonable grounds to doubt the identity of the natural person making a request pursuant to Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject. This is clear from Article 12(6).

Under Article 15, the data subject has the right to obtain from the controller a copy of the personal data processed by the controller. The data subject shall also receive other information, such as the purpose for which the personal data are processed and to which recipients or categories of recipients the data are disclosed.

The European Data Protection Board (EDPB) Guidelines 01/2022 on access indicate that the calculation of the one month deadline in Article 12(3) is calculated from the date of receipt of the request. However, where, following the request, a controller needs to take measures to ensure the identity of the data subject, the time limit may be suspended until the controller has received the information necessary to identify the data subject. This provided that the request for additional information has been made without undue delay.

Assessment of the Authority for Privacy Protection (IMY)

The investigation shows that the complainant's request for access was made on 6 June 2021 and that Klarna met the request on 12 July 2021, i.e. approximately one month later. It is also apparent that Klarna had doubts as to whether it was indeed the appellant who made the request and therefore, on 11 June 2021, asked the appellant to supplement the request with information for the purpose of verifying its identity and reminded it on 24 June 2021.

IMY considers that Klarna had reasonable grounds to doubt the identity of the appellant and has adequately requested proportionate information without undue delay. Since the complainant did not submit that information until 24 June 2021, the time limit did not start to run again until then. Furthermore, IMY considers that Klarna has handled the request without undue delay through the total 23 days.

IMY concludes against this background that the investigation in the case does not show Klarna has processed the complainant's personal data in breach of Articles 12(3), 12(6) and 15 of the GDPR.

The case is hereby closed."

Appeal Notice

Against this decision a lawsuit before the Verwaltungsgericht Berlin (administrative court of Berlin), Kirchstraße 7, 10557 Berlin is admissible. The lawsuit needs to be filed in written form within one month after the announcement of this decision, it can also be filed as an electronic document with a qualified electronic signature (QES) for the record of the clerk of the court. Please, note that in case of filing the lawsuit in writing the legal deadline is only met if the lawsuit reaches the administrative court within the deadline.

The Berlin Commissioner for Data Protection
and Freedom of Information

Baden-Württemberg
THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 ·D-70025 Stuttgart

[redacted]

Fine proceedings for violation of Articles 5, 6, 17 of the GDPR due to publication of personal data on the internet without consent and non-compliance with the erasure request

Decision

The fine proceedings shall be terminated in accordance with Section 47(1)(1) of the Act on regulatory offences.

Findings:

I.

[redacted], an association for the protection of the marine environment, conducted in 2010 a "Petition to stop the consumption of whale meat in the Faroe Islands". Supporters were able to sign the petition online, giving their name and country, and leave a comment. A total of 57,281 people signed the petition, which was published on the Internet at [redacted] with the names of the supporters. On the other hand, representatives of the Faroe Islands were given a printout of the petition together with the signatures. The petition was closed on 26 July 2010.

On 16 July 2015, [redacted] from the United Kingdom, who had signed the petition online, contacted the managing sole shareholder of the entity with the request that her signature, which was still available under [redacted] and thus freely accessible via the internet, be removed from the list of signatures. In addition to the name of the complainant, the names of all signatories to the petition were available via the following links:

[redacted]

In addition, the previously listed Internet pages were indexed at Google, so that a Google search of a person listed there also listed the Internet page with the petition as a search result. Accordingly, in a Google search for the complainant, the page [redacted] was linked as fourth hit at Google.

The complainant's request was not complied with by [redacted] with the explanation that the complete list of signatures had already been removed from the website years ago. On 29 April 2019, the complainant again turned to [redacted] with the same request, which was rejected with the same reasoning as before. In fact, however, the relevant link was still accessible, as an entry of the link in a web browser would have revealed.

Subsequently, the complainant lodged a complaint with the UK supervisory authority, which initiated IMI Article 56 proceedings on 26 August 2019 (IMI no. 74456.1) due to the company’s registered office in Baden-Württemberg. The Baden-Württemberg DPA accepted to handle the case as LSA. In the course of the hearing by the LSA, [redacted] again - erroneously - stated that the signature list had already been deleted and the erasure request had thus been fulfilled.

As a result, the LSA initiated fine proceedings against [redacted] on suspicion of violation of the requirement to storage limitation pursuant to Article 5(1)(e) of the GDPR as well as violation of the obligation to erasure pursuant to Article 17(1) of the GDPR, and heard [redacted] on this matter in a letter dated 16 November 2020. In addition to the list of signatures relating to the complainant, the subject of the fine proceedings was also a list of signatures published under

[redacted] dated 1 May 2008 with the names and places of residence of 1,294 persons, which had already been closed on 30 April 2008 and handed over to a representative of the Federal Government in Berlin.

In a letter dated 24 November 2020, [redacted] stated that the list of signatures from 1 May 2008 should not be deleted, as the underlying campaign had not yet ended due to lack of success. Furthermore, they stated that the signature list from 2010 concerning the complainant had already been deleted ten years ago, although there had been no corresponding confirmation from [redacted]. Accordingly, they stated that the signature list was also not available on the website. Screenshots of the provider were submitted as proof, which in fact only showed the editor of the navigation bar of the homepage of [redacted]

In a letter dated 15 January 2021, [redacted] was once again informed of the legal situation and the continuing obligation to erasure. [redacted] was given a final opportunity to delete the signature lists, together with the announcement of a chargeable erasure order and a final decision in the fine proceedings.

Subsequently, [redacted] demonstrably deleted the corresponding signature lists from its homepage, so that a Google search for the complainant no longer refers to the [redacted] homepage and the signature list there *[Please find the respective screenshots in the relevant documents].*

II.

The fine proceedings shall be terminated for reasons of expediency pursuant to Section 47(1)(1) of the Act on regulatory offences.

It is true that [redacted] at least negligently violated Article 5(1)(e), Article 6(1) and Article 17(1) of the GDPR by publishing the names of the data subjects on the homepage years after the signature campaigns had ended without their consent and by not deleting them despite a request to do so.

The corresponding violation is, in principle, also serious, as a large number of persons were affected by the unlawful publication, the corresponding publication lasted

for a period of ten resp. twelve years and [redacted] did not comply with the request for erasure even despite repeated requests by the complainant and the LSA.

Nevertheless, it is possible to refrain from imposing a fine in exceptional cases. First of all, it must be seen that [redacted] is a non-profit and thus not commercially active company which, apart from the managing sole shareholder, has no employees and is dependent on donations for its non-profit activities, which in 2020 amounted to only 10,603.00 Euros up to the time of the statement of 24 November 2020. In addition, [redacted] did not act intentionally, but on the contrary, due to a lack of technical expertise, was convinced that the signature list had already been deleted and had thus complied with the complainant's request for erasure. Finally, [redacted] restored the lawful state by fulfilling the complainant's request for erasure, albeit with a delay of several years and at the repeated request of the LSA.

In view of the nature of fines as a remedial measure, as an exception, punishing [redacted] by imposing a fine does not appear necessary, so that the fine proceedings are terminated for reasons of expediency. However, in case [redacted] will violate data protection regulations again, they will have to expect the imposition of a fine, which will then not be insignificant.

[…]

Baden-Württemberg

THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 ·D-70025 Stuttgart

[redacted]
[...]

File No. R 1257/35

Complaint of [redacted], R 1257/35

Dear Madam or Sir,

Having examined the facts of the case we get back to you regarding the complaint under the above-mentioned Ref. no.

I. The course of the procedure

The Baden-Wuerttemberg DPA (hereinafter: BW DPA) launched an investigation based on the complaint of [redacted] (hereinafter: the Complainant) pursuant to Article 57(1)(f) of the General Data Protection Regulation (hereinafter: GDPR).

In July 2019, the Complainant lodged a complaint with the Data Protection Authority of DE/Hesse, in which he presented that he had been traveling with a tour group and that the first hotel in Riga ([redacted]) did not ask for an individual entry in a registration form, but this had to be entered with all personal data (including date of birth and passport number) in a collective form. This allowed all travelers to see the data of all the other guests. The tour guide said that this was common practice. However, such registration forms were not used for the other overnight stays.

The DPA DE/Hesse submitted the complaint to our DPA (DE/BW), after the Latvian DPA stated that the controller as per Article 4(7) GDPR regarding such processing would not be the hotel group ([redacted]), but the tour agency, being the distributor of the tourist declaration list. The tour agency is [redacted] DE/BW.

On 5 November 2020, the DE/BW DPA initiated a procedure to establish the lead supervisory authority in accordance with Article 56 of the GDPR (IMI no. 161583), as the Latvian DPA was assumed to be in fact the lead supervisory authority. This was according to the statements of the tour agency from 24 July 2020 that the hotels are in charge of the tourist lists themselves, in particular to meet local legal requirements of the hotel *[for details we refer to the response letter from* [redacted] *in IMI].* The Latvian DPA however refused to handle the case as LSA, following the contrary statements of [redacted] that the tour agency is the controller.

After some discussions on that matter, the DE/BW DPA agreed to handle the case as LSA and created a case register in IMI (no. 179802).

In IC 398883, our intended draft decision has been shared with the CSAs to collect their views on it, before submitting it formally.

As we did not receive any comments in the IC from the CSAs, we presented the draft decision to the CSAs as per Article 60(3) GDPR (IMI no. 430639). This procedure has been closed without a reasoned and relevant objection or other comments from the CSAs.

II. Facts of the case

The complainant states that during a vacation with a tour group, in the first hotel in Riga ([redacted]), he was asked to enter his personal data, such as date of birth and passport number, in a list on a registration form. The hotel did not ask for an individual entry in a registration form, but this had to be entered with all personal data (including date of birth and passport number) in a collective list. This allowed all subsequent travellers to see the data of all the other guests. The tour guide said that this was common practice. However, such registration forms were not used for the other overnight stays.

On 17 June 2020, the DE/BW DPA contacted [redacted] in order to ask them for a response to the facts the complainant presented. [redacted] replied to our DPA not to have an oversight and influence on the data processing in this context, as employees of the hotel would carry out the data processing independently.

In addition, [redacted] stated to our DPA that they have completely ceased its activities as a tour agency as of October 31, 2020.

III. The findings of the Authority

Considering [redacted] to be the controller in regards to the relevant data processing, as their influence on the purposes and means of the processing (Art. 4(7) GDPR) can not be ruled out, the

DE/BW DPA reiterates that data must be stored in such a way that unauthorized persons - including other guests - cannot access the data of the individual registered guests. The completed paper forms, for example, must therefore not be left lying around openly on the counter and should be kept securely locked away at the end of the working day. It must also be prevented that other guests see the data of the pre-registered persons from the group.

Making the data of pre-registered persons from the tourist group available and visible to the subsequent guests by using a collective registration list **constitutes a violation** of the important principle of integrity and confidentiality as defined in Art. 5 GDPR. According to Art. 5(1)(f) GDPR, personal data shall be 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 (Art. 32 GDPR). According to Art. 5(2) GDPR, the controller shall be responsible for, and be able to demonstrate compliance with, the conditions set out in Art. 5(1).

Therefore, travel agencies have to use themselves and/or to instruct their respective travel partners, e.g. hotels, to use individual forms or even electronic recording to make sure that the data processing takes place in line with Art. 5(1)(f) GDPR.

IV. Legal consequences

The DE/BW DPA establishes that [redacted] **breached Article 5(1)(f) in conjunction with Art. 32 GDPR as well as Art. 5(2) GDPR.**

Hence, the DE/BW DPA issues a **reprimand** to the company for the abovementioned infringements of the GDPR, based on **Article 58(2)(b) GDPR.**

The DE/BW DPA will also reiterate to the company again the fact that data processing relating to travel guests must be carried out in a way that respects the integrity and confidentiality of the guests' data and that the controller must implement measures and processes to comply with that provision, as stated above.

Due to the constellation that [redacted] has assured to the DE/BW DPA that it has ceased to operate as a tour agency as of October 31, 2020, the DE/BW DPA desists from making use of further corrective powers and hereby close the procedure. The DE/BW DPA also informed the complainant about these facts and did not receive an objection or other response to that from him.

V. Information on legal remedies

An appeal against this decision may be filed in writing, electronically or for recording with the Administrative Court of Stuttgart, Augustenstraße 5, 70178 Stuttgart, within one month of notification pursuant to Article 78 of the General Data Protection Regulation in conjunction with Section 20(1) and (3) of the Federal Data Protection Act.

Bayerisches Landesamt für
Datenschutzaufsicht

Bayerisches Landesamt für Datenschutzaufsicht | Postfach 606 | 91511 Ansbach

[redacted]

UNOFFICIAL TRANSLATION

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18 | 91522 Ansbach
Tel: 0981 180093 0
Fax: 0981 180093 800
E-mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Your contact person
[redacted]

Your sign/letter of	**Our reference number**	
04/05/2021	LDA-1085.2-5489/21-VW	Ansbach, 04/12/2023

Data protection complaint pursuant to Art. 77 General Data Protection Regulation (GDPR)

Your complaint against [redacted] – Final decision

[redacted]

We come back to your data protection complaint, conducted with us under the reference above, against [redacted] ([redacted]) (controller).

1. Summary of your complaint

In your complaint, you have asserted a breach of your right of access by the controller. You indicated that on 29/03/2021, you sent a request for information to the controller and that you had not received a reply by 04/05/2021. Your complaint was accompanied by a document dated 29/03/2021, in which you request information from the controller.

2. Handling of your complaint

By e-mail of 10/05/2021, we confirmed receipt of your complaint and pointed out that your complaint is a so-called cross-border processing pursuant to Art. 4 No. 23 GDPR, as the main establishment of the controller is located in France. We further pointed out that for this reason, a joint processing of your complaint will take place by the lead data protection supervisory authority and the data protection supervisory authorities of all other Member States affected by this processing in the European Economic Area (EEA). Finally, we informed that, according to our findings, the French Data Protection Authority (Commission Nationale de l'Informatique et des

Libertés – CNIL) is lead supervisory authority and that we forward your complaint to it and to the other supervisory authorities concerned.

By e-mail of 21/06/2023 we informed you about the feedback received by the CNIL in the meantime. The CNIL had asked the controller to comment in writing. The controller proved that on 07/05/2021 a request for information dated 05/05/2021 had been received from you, which was answered on 25/05/2021. The relevant documents were attached to our e-mail dated 21/06/2023. We gave you the opportunity to comment on this by 21/07/2023. We have not received any feedback from you.

3. Legal evaluation and outcome

In the light of the above, your complaint is dismissed pursuant to Art. 60 (8) GDPR. There is no breach of data protection by the controller, in particular the provisions of Art. 12 (3), Art. 15 GDPR. In particular, the data controller responded to your request for information within the time limit provided by law.

We hope to have made our decision comprehensible to you. If you do not agree with this, the administrative legal process is open to you. Please refer to the following instructions on appeal.

We hereby conclude the procedure under the above reference number and remain

Sincerely,

[redacted]

This letter has been sent by machine and is valid without signature.

Legal notice

With reference to Articles 77 and 78 of the GDPR, we would like to point out that you may file a lawsuit against this decision at the

Bayerisches Verwaltungsgericht Ansbach in 91522 Ansbach,

Promenade 24 – 28, 91522 Ansbach

Information on the legal notice

The lawsuit may be lodged in writing, for minutes or electronically in a form authorised to substitute the written form. The filing of an appeal by simple e-mail is not allowed and has no legal effects!

As of 01/01/2022, the group of persons referred to in § 55d VwGO (in particular lawyers) must in principle file legal proceedings electronically.

In proceedings before the administrative courts, a procedural fee is due as a result of the action being brought.

Our reference: LDA-1085.1-2300/20-F
IMI Art. 61: 185779
IMI draft decision: 591896

Controller: [redacted] (publ)

On the basis of the draft decision of the Swedish Integritetsskyddsmyndigheten (SWE DPA) No. 591896, the Data Protection Authority of Bavaria for the Private Sector (BayLDA) pursuant to Article 60(8) of the GDPR issues the following

Final Decision:

The complaint is rejected.

Justification:

The complaint was received by the BayLDA on 02.03.2020 and was forwarded via IMI to the SWE DPA as the lead data protection supervisory authority for the controller.

On 02.01.2024, the SWE DPA submitted the draft decision no. 591896 to the concerned supervisory authorities with the following contents:

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that the investigation has not shown that [redacted] has processed the complainant's personal data in breach of Article 6(1) of the General Data Protection Regulation in the manner alleged in the complaint.

The case is closed.

Report on the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated an audit towards [redacted] (the company or [redacted]) due to a complaint. The complaint has been submitted to IMY, as a supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation from the supervisory authority in Germany where the complainant has lodged their complaint in accordance with the GDPR's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through written correspondence. On 10 of November 2023, IMY sent a request for information to [redacted], in order to ascertain whether [redacted] was the controller of the processing in question and, if so, under which legal basis under Article 6(1) of the GDPR the applicant's personal data had been processed.

Since this is a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned has been the data protection authorities in Germany, The Netherlands, Norway, France, Finland and Denmark.

The complaint
In its complaint, the complainant essentially stated the following. The complainant made two attempts to purchase an online service on 26 August 2019. The complainant used [redacted] as a payment solution. The complainant made a third attempt to purchase the online service on 2 September 2019. The complainant used [redacted] as a payment solution on this occasion as well. This purchase went through. [redacted] subsequently invoiced the appellant for two purchases, even though only one purchase was successful. [redacted] then forwarded the complainant's personal data to a debt collection agency. According to the complainant, [redacted] did not have the right to process her personal data in the way that it did.

What [redacted] has stated
[redacted] has mainly stated the following. In its statement dated 24 November 2023, [redacted] has stated that it cannot identify the complainant with the information available from the complaint and that it is therefore unable to answer the questions in IMY: s supervision letter, unless they receive more information.

On 28 November 2023, IMY contacted [redacted] by telephone to find out what additional information [redacted] needed to be able to identify the complainant. [redacted] replied that they needed information about the email address with which the purchase had been made.

On 29 November 2023, IMY communicated [redacted]'s response to the concerned national supervisory authority in the country where the complainant filed the complaint (Germany) and asked them to contact the complainant in order to obtain the requested email address.

On 21 December 2023, the national supervisory authority (Germany) returned with the information that the complainant had not returned.

Justification of the decision

It follows from Article 57(1)(f) of the GDPR that Swedish Authority for Privacy Protection (IMY) must deal with complaints from data subjects who believe that their personal data is being processed in a way that is contrary to the GDPR. The provision also states that IMY shall, where appropriate, investigate the subject matter of the complaint. The Court of Justice of the European Union has stated that the supervisory authority shall investigate such complaints with due diligence. (Schrems II, case C-311/18, EU:C:2020:559, para. 109.)

According to Section 23 of the Swedish Administrative Procedure Act (2017:900), an authority shall ensure that a case is investigated to the extent required by its nature.

IMY: s audit concerns whether [redacted], as data controller, has processed the complainant's personal data without a legal basis in Article 6(1) of the General Data Protection Regulation. [redacted] has not been able to answer IMY: s questions concerning the processing of the complainant's personal data in the light of the fact that they have not been able to identify the complainant. The complainant has been given the opportunity to supplement [redacted] complaint with information about the e-mail address used for the purchase in question.

IMY considers that the matter has been investigated to the extent required by Article 57(1)(f) of the General Data Protection Regulation and Section 23 of the Swedish Administrative Procedure Act. IMY notes that there is no basis in the investigation to conclude that [redacted] processed the complainant's personal data without a legal basis in Article 6(1)(f) of the GDPR.

The case is closed.

As the concerned supervisory authorities (including BayLDA) did not object to this draft decision, the BayLDA hereby adopts this draft decision as final decision in accordance with Article 60(8) of the GDPR.

Ansbach, 20.02.2024

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

521.13446
631.345
CR 52519
DD 186058

FINAL DECISION

Berlin, 26 April 2021

OUTFITTERY GmbH
Management Board
[redacted]
Leuschnerdamm 31
10999 Berlin

For information:
ISiCO Datenschutz GmbH
[redacted]
Am Hamburger Bahnhof 4
10557 Berlin

Reprimand
Complainant: [redacted]
Your letter of 18 December 2020 (Your ref IS-0472-10)

Dear [redacted],

We hereby issue a reprimand to your company for a violation of the General Data Protection Regulation (GDPR).

Reasoning:

This decision is based on the following considerations

I.
The Berlin DPA has established the following facts:

The above-mentioned complainant maintained a customer account with Curated Shopping GmbH, which was taken over by Outfittery GmbH on 27 June 2019, under his email address [redacted - email address 2] and another customer account with Outfittery GmbH under the email address [redacted - email address 1]. By email from the address [redacted - email address 1], the complainant requested Outfittery GmbH to erase his data on 30 December 2019 and mentioned his user account set up under the email address [redacted - email address 2] in his erasure request.

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.

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/beschwerde.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

be Berlin

You confirmed the erasure of the complainant's data in an email sent to his email address [redacted - email address 2] on 2 January 2020. On 16 September 2020, the complainant again received an advertising letter from Outfittery GmbH by post. In the above-mentioned statement, you stated that on 2 January 2020, the complainant's existing customer account at the e-mail address [redacted - email address 2] had been deleted and admitted that due to an employee error, however, his other customer account with the e-mail address [redacted - email address 1] had not been erased.

II.
Legally, we assess the facts of the case as follows. Your company has violated the GDPR.

According to Article 5(1)(a) GDPR, personal data must be processed in a lawful manner. In order for processing to be lawful, personal data must be processed either on the bases of the consent of the data subject concerned or some other legal basis, according to sentence one of Article 6(1) GDPR. Pursuant to Article 17(1)(a) GDPR, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

Through his erasure request of 30 December 2019 pursuant to Article 17(1) GDPR, the complainant has expressed that he is not interested in continuing the customer relationship with Outfittery GmbH. Further processing of his data for the business purposes of Outfittery GmbH was therefore no longer necessary. Nor was the erasure request barred for other reasons.

However, his erasure request was not fully implemented due to an internal employee error at Outfittery GmbH. Admittedly the data assigned to the customer account with the email address [redacted - email address 2], was erased by Outfittery GmbH on 2 January 2020. However, the erasure of the data assigned to the customer account with the email address [redacted - email address 1] did not take place. This data continued to be stored in the systems of Outfittery GmbH and was used again by sending the postal advertising letter that the complainant received on 16 October 2020, although it should have already been erased based on his previous request for erasure.

The fact that Outfittery GmbH did not fully implement his deletion request of 30 December 2019 due to an internal employee error is irrelevant, as Outfittery GmbH must ensure compliance with its data protection obligations by taking appropriate technical and organisational measures in accordance with Article 24(1) GDPR. In any case, Outfittery GmbH could also be expected to take internal organisational measures to ensure that the request for deletion was processed in accordance with data protection laws.

The continued use of the complainant's data and its continued storage were therefore without legal grounds.

Outfittery GmbH thus violated Articles 5(1)(a), 6(1), 17(1) and 24(1) of the GDPR.

III.
As a result, we have decided not to take any further supervisory measures due to the violation, but to leave it at a reprimand.

The reprimand is based on Article 58(2)(b) GDPR.

Taking into account the specific circumstances of the case under investigation, we consider a reprimand to be appropriate after completion of our investigation. We have again established a violation on your part

In the safe expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Kind regards,

[redacted]

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 24 March 2021

535.1660
631.257
CR 126887
DD 156313
FD 188955

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.

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

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** AWIN AG (www.awin.com)
- **Incident**: vulnerability in API interface
- **Date of occurrence**: unknown (at the earliest in 2017)
- **Date of acknowledgement of the incident**: 20 March 2020
- **EU/EEA Member States concerned, with the number of data subjects concerned**: total of 309
    - Austria: 2
    - Belgium: 4
    - Denmark: 4
    - France: 17
    - Germany: 106
    - Hungary: 2
    - Ireland: 3
    - Italy: 7
    - Netherlands: 22
    - Norway: 2
    - Poland: 5
    - Portugal: 2
    - Spain: 7
    - Sweden: 7
    - UK: 119
- **Category of data subjects**: customers
- **Category of the data types/data records concerned**: email addresses (no passwords)
- **Likely consequences of the violation of the protection of personal data**: misuse

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

Via an API interface, the above-mentioned personal data could be retrieved for a part of the customer data records. By repeatedly calling up the interface with different search parameters, it was possible to retrieve the personal data of all customer accounts.

be Berlin

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)

Immediately after the data leak became known, the corresponding API interface was restricted in such a way that the aforementioned personal data could no longer be retrieved. The data leak was thus permanently closed.

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

All data subjects were informed of the incident by e-mail.

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

Not relevant. However, access to the API interface was also previously transport-encrypted.

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 point 3

7. Measures taken by the LSA Berlin DPA

7.1 Measures taken 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 Measures taken regarding data protection violations beyond Articles 33, 34 GDPR

As regards this point as well, the Berlin DPA closes the case, since the data was mainly not sensitive and the underlying technical problem has been solved.

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

631.284
535.1963
A56ID 161003
CR 169740
DD 175403

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.

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

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller**: Springer Nature AG & Co KgaA
- **Incident:** 411 author data (names, partly also e-mail addresses) were inadvertently forwarded to the platform Research Square without the consent of the data subjects and partly published there. The author data of 36 of 76 research papers were published for 25 days.
- **Date of occurrence**: 11 July 2020
- **Date of acknowledgement of the incident:** 4 August 2020
- **EU/EEA Member States concerned, with the number of data subjects concerned:** Austria, United Kingdom, Germany, France, Italy, Estonia, Belgium, Netherlands, Sweden, Finland. The exact number of affected persons per country would require a recreation of the breach. For this reason, it was decided not to do so. Please find a list of the institutions concerned attached.
- **Category of data subjects:** 411 author names of scientific papers and e-mail addresses in some cases.
- **Category of the data types/data records concerned:** 80 datasets with bibliographic data of scientific papers.
- **Likely consequences of the violation of the protection of personal data:** almost none since the controller also published the data in their scientific journals that are available digitally (partly for free) and on paper for free for the scientific community through (university) libraries.

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

Due to an administrative error (a faulty system configuration), 411 author data (names, partly also e-mail addresses) were forwarded to the platform Research Square and partly published there.

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 controller has taken the following measures:

- corrected incorrect system configuration;

be Berlin

- deactivated the publication of the data on the Research Square platform and erased all data transmitted to the platform without authorisation (the platform has an access point where controllers such as Springer can edit the data you have entered);
- developed a concept to minimize the risk of data transmissions being influenced by system configurations;
- revised quality assurance, especially for updates.

The Berlin DPA assess the measures as sufficient and effective.

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

Notification of the data subjects is not mandatory, as there is no high risk. No sensitive data have been published. In addition, the names of the authors were and are intended for publication in the journals "Breast Cancer Research" and “Critical Care”.

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

Not applicable.

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 3.

7. Taken measures by the LSA Berlin DPA

In the light of the above-mentioned considerations, the Berlin DPA closes the case as only a limited amount of uncritical data was affected. This data was meant to be published in another place and has been published there by now.

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin DPA: 521.11398 / 632.208
Spanish DPA: E/04491/2019
IMI CR: 72181
DD 329643

Final Decision

Attorney at Law
[redacted]
Sieglindestraße 7
12159 Berlin

Reprimand
Your letter of 4 September 2020
Our hearing of 21 June 2021

Dear [redacted],

We hereby issue a reprimand to your client for a violation of the General Data Protection Regulation (GDPR).

Reasoning:

Our decision is based on the following considerations:

I.
We have established the following facts:

On 9 January 2019, the complainant sent an unsolicited application with her CV to info@secretaria.es. On the same day, as well as on 15 January 2019, she received an email from [Person 1] informing her that she had received the complainant's application for the company CLBS in Thailand. She did not reply as she assumed they were fraudulent emails. The complainant then received a call from [Person 1] on 21 January 2019. [Person 1] advised that she had received the data from the unsolicited application to secretaria.es. On 21 January 2019, the complainant therefore sent an email to dataprivacy@secretaria.es requesting access to her data and its erasure. The complainant did not receive a reply.

The email address info@secretaria.es is the general contact address of Deutsche Bureau AG's customer service. Deutsche Bureau AG is a wholly-owned subsidiary of ebuero AG, which is also based in Berlin, Germany. Deutsche Bureau AG provides telephone secretarial and business centre services for customers in several EU member states. This also includes permanent activity on the Spanish market, where the company offers its services under the domain secretaria.es as well as by means of Spanish telephone numbers and Spanish-speaking employees. For this purpose, Deutsche Bureau AG uses, among others, Chiangmai Lanna Business Services Ltd. ("CLBS"). CLBS, which is based in Thailand, is also a wholly-

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.

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/beschwerde.html

For all o her 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

be Berlin

owned subsidiary of ebuero AG and operates for the other parts of the group of companies on the basis of order processing agreements supplemented by EU standard contractual clauses.

Customer service requests to info@secrataria.es are processed on behalf of Deutsche Bureau AG by employees of CLBS as a processor. The complainant's e-mail was therefore opened and processed by an employee of CLBS. The employee forwarded the e-mail to the internal recruiting department of CLBS. In doing so, he assumed that he was acting in the complainant's interest. We were provided with a copy of the underlying data processing agreement and the signed standard contractual clauses.

After the hearing was received by Deutsche Buero AG, CLBS employees were once again instructed not to forward incoming applications and application documents internally for recruiting purposes without the sender's consent.

Deutsche Bureau AG has stated that the complainant's data has since been erased. It was therefore no longer possible to establish whether the request for information had been answered or whether the erasure had been confirmed.

II.
Legally, we assess the facts of the case as follows: Your client has committed a violation of the General Data Protection Regulation (GDPR).

There has been a violation of Article 6(1) GDPR by Deutsche Bureau AG, as there was no legal basis for the further processing of the application documents. CLBS processed personal data on behalf of Deutsche Bureau AG in accordance with Article 28 GDPR. Deutsche Bureau AG has concluded a data processing agreement with CLBS for this purpose. Deutsche Bureau AG remains responsible for the processing of the data. For the export of the data, the companies have concluded the standard contractual clauses issued by the EU. The processing of personal data on the basis of these contracts is permitted under the GDPR. Accordingly, an employee of CLBS was allowed to receive the application documents. However, the complainant applied to secretaria.es and thus directly to Deutsche Bureau AG. Her documents should therefore have been forwarded only to the competent persons at Deutsche Bureau AG. There is no legal basis for forwarding them within CLBS. The documents should not have been examined in more detail there, nor should [redacted] have been allowed to contact the complainant by e-mail or telephone.

Furthermore, there is a violation of Articles 15(1), 17(1) and 12(1) and (3) GDPR, as the erasure request of 21 January 2019 was not answered within one month. It is true that the application documents have been erased in the meantime. However, Deutsche Bureau AG should have responded to the request within one month, which it did not do.

III.
As a result, we have decided not to take any further supervisory measures due to the violation, but to leave it at a reprimand for the time being.

The reprimand is based on Article 58(2)(b) GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after completing our investigation. We have identified a violation on the part of your client for the first time. When we approached your client, she was reasonable and once again instructed the employees of the processor not to forward application documents internally.

In the certain expectation that your client will comply with the data protection regulations in the future, we consider the matter closed.

Legal remedy
An action against this decision may be brought before the Berlin Administrative Court. It must be filed in writing - also as an electronic document using a qualified electronic signature (QES) - or with the clerk of the court within one month of notification of this decision at the Berlin Administrative Court, Kirchstraße 7, 10557 Berlin. It is pointed out that if the action is filed in writing, the time limit for filing an action is only met if the action is received by the Administrative Court within this time limit.

Kind regards,
[redacted]

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin DPA: 521.10949 / 632.201
French DPA: 18022379
A56ID 60758
CR 63286

Final Decision

Berlin, 7 June 2021

[redacted]

For your information:
[redacted]

Reprimand
Complainant: Mr [redacted]
Your letters of 30 April 2019 and 27 November 2020

Dear Sir or Madam,

The Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA) hereby issues a reprimand to your company for a violation of the General Data Protection Regulation (GDPR).

Reasoning

The decision is based on the following considerations:

I.
The Berlin DPA has established the following facts:

In a message dated 29 April 2018, the complainant requested [redacted] to erase his personal data and to close his customer account. The erasure was confirmed to the complainant by [redacted] in an email dated 30 April 2018. In his complaint of 8 November 2018, the complainant submitted that a few months after the erasure had been confirmed to him, he had received an email from [redacted] informing him that the email address of his customer account had been changed. The complainant then confronted [redacted] by e-mail with the fact that his customer account should have been erased long ago. The customer account was finally erased by [redacted] on 26 March 2019.

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.

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

be Berlin

In the statement of 30 April 2019, you informed us that the non-erasure could possibly be related to the reorganisation of internal processes with regard to the applicability of the GDPR. The erasure of the customer account on 26 March 2019 had been carried out due to a query with the customer service department by the legal department in an entirely hasty manner and without consultation by the customer service department. However, the fact that the account was not initially deleted could possibly be due to the fact that there were obstacles. However, it is no longer possible to clarify the facts of the case because the customer account has been erased. [redacted] is of the opinion that the facts of the case should be assessed solely according to the old legal situation.

In the statement of 27 November 2020, you described the procedure in the event of a deletion request. Before erasure, it is always checked whether there are obstacles such as open orders or open invoice amounts. If this is not the case, the customer account is first deactivated and then erased. Otherwise, the customer would be informed about the existence of the specific reason for obstruction. Furthermore, you pointed out that the display of the data in Annexes 3 and 4 (Annex 3:[redacted]_hacking and Annex 4: [redacted]_question) differed from the display of the data in Annexes 1 and 2 (Annex 1: [redacted]_contact and Annex 2: [redacted]_answer), so that, depending on how the data was read (DD/MM/YY or MM/DD/YY), it was also possible that the e-mail address in the customer account had been changed before the request for deletion. In this respect, a manipulation by the complainant could not be ruled out. Before the erasure, a check by the customer service had shown that there were no indications of fraudulent activities.

II.
Legally, we assess the facts as follows. Your company has committed a violation of the General Data Protection Regulation.

1. <u>Violation of Article 17(1)(a) and (b) GDPR.</u>

The failure to erase the complainant's customer account constitutes a violation of Article 17(1)(a) and (b) in conjunction with Article 6(1), Article 5(1) GDPR.

The GDPR applies in the present case, as the failure to erase or, in a similar way, the continued storage of the complainant's data is data processing which, although it started before the GDPR applied, was still ongoing on 25 May 2018 and beyond. The complainant's request for erasure was made on 29 April 2018 and thus before the GDPR applied. However, it is undisputed that the complainant's request was not complied with until 26 March 2019, i.e. after the deadline. The supervisory complaint was lodged on 8 November 2018 and thus also after the effective date.

With the applicability of the General Data Protection Regulation, the national law of the Member States ceased to apply. Pursuant to Article 99(2) GDPR, the General Data Protection Regulation has been directly applicable since 25 May 2018 (effective date). Data processing that started before 25 May 2018 and continued beyond 25 May 2018 must comply with the requirements of the General Data Protection Regulation as of the effective date (cf. recital 171 pp. 2; Taeger/Gabel/Golland, GDPR, 3rd ed. 2019, Article 99 marginal no. 5; cf. also FG Saarland, decision of 03.04.2019, Ref: 2

K 1002/16 = DStRE 2019, 1226, marginal no. 10). The lawfulness of data processing as of 25 May 2018 must therefore be assessed in accordance with the GDPR, even if it began before the effective date.

Pursuant to Article 17(1) GDPR, if one of the listed grounds applies, the data subject has 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. If one of the grounds pursuant to Article 17(1) GDPR applies, the controller is also obliged to erase the data immediately, irrespective of the data subject's request. Erasure is immediate if it takes place without undue delay.

Article 17(1)(a) to (c) GDPR concern cases in which initially lawful data processing has become unlawful (BeckOK/Worms, Datenschutzrecht, 34th ed., Article 17 GDPR, para. 24). In the present case, it is assumed that the data processing based on the customer relationship was initially lawful within the meaning of Article 6(1) and Article 5(1) GDPR.

However, with the declaration of the request for erasure on 29 April 2018, the purpose of processing ceased to exist (Article 17(1)(a) GDPR). Accordingly, a reason for erasure exists if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. If a customer relationship is terminated, the data processing is usually no longer necessary (cf. Paal/Pauly/Paal, GDPR, 3rd ed. 2021, Article 17 marginal no. 23). By requesting the closure of the customer account, the complainant initiated the end of the customer relationship, so continued storage of the data was no longer necessary within the meaning of Article 6(1)(b) GDPR.

Insofar as the processing was based on consent, the reason for deletion pursuant to Article 17(1) (b) GDPR also exists. Accordingly, the personal data must be deleted if the data subject withdraws consent and there is no other legal basis for the processing. The request for erasure implicitly includes the withdrawal of consent within the meaning of Article 7(3) sentence 1 GDPR (Sydow/Peuker, GDPR, 2nd ed. 2018, Article 17 marginal no. 20). The erasure request continues to apply from the day of the declaration until the day of fulfilment of the claim, so that regardless of the old legal situation, you were in any case obliged to erase without delay from the effective date of 25 May 2018 in accordance with Article 17(1)(b) GDPR. In view of the change in the legal situation, the complainant did not have to reissue his request for deletion, as the legal basis Article 6(1)(a) GDPR had ceased to exist. Notwithstanding the fact that Article 17(1) GDPR does not require a request anyway, as there is an obligation to delete regardless of the request, such a requirement would disadvantage the data subject if the request for deletion was - as in this case - unjustifiably not complied with. This would contradict the protective purpose of the data subject's rights.

In any case, the retention of the complainant's data in the period between 25 May 2018 and 26 March 2019 (date of erasure) is also not permissible in any other way pursuant to Article 6(1) GDPR.

As explained, Article 6(1)(a) GDPR cannot be considered as a legal basis, as the consent was in any case withdrawn in an implied manner by the request for erasure.

Furthermore, the retention of the personal data cannot be based on Article 6(1)(f) GDPR, as there was no overriding legitimate interest in not erasing

the data. The interests can be of a legal, economic or non-material nature (BeckOK Daten-schutzR/Albers/Veit GDPR, 34th ed., Article 12 para. 18). The controller bears the burden of proof for the existence of the conditions for data processing and thus for the existence of legitimate interests (cf. also Gola/Schulz, GDPR, 2nd ed. 2018, Article 6 marginal no. 7). [redacted] has not demonstrated legitimate interests in the form of the existence of obstacles. The mere possibility that grounds for obstruction might have existed does not constitute proof.

Furthermore, there are no actual indications for the existence of grounds for obstruction, e.g. in the form of outstanding invoices, which would have to be taken into account in the context of Article 6(1)(b) GDPR anyway. This view is supported by the fact that the hasty erasure on 26 March 2019 would probably not have taken place if reasons for the failure to erase the data at that time had been apparent to the customer service when re-examining the process. Rather, the hasty catching up of the erasure suggests that the customer service recognised its own omission in this respect and attempted to rectify it. Furthermore, [redacted] states in its submission of 27 November 2020 that, as a matter of principle, a review of the grounds for obstruction takes place as a standard procedure prior to every erasure. Why such a check should not have taken place in this case, of all cases, is not explained. The confirmation of erasure sent to the complainant on 30 April 2018 is rather an indication that the conditions for erasure already existed at that time.

Finally, you cannot successfully invoke one of the exceptions under Article 17(3) GDPR. In this respect, only Article 17(3)(e) GDPR applies. There were no indications that you or the complainant would need the data for the assertion, exercise or defence of legal claims at the time of the request for deletion. The facts of the case could no longer be determined in detail because the erasure was carried out too quickly. Insofar as you have put forward the existence of obstacles as a possible reason for non-erasure, the mere theoretical possibility is not sufficient to fulfil the exceptional circumstances. As already explained, there are no factual indications for the existence of obstacles.

2. <u>Violation of Article 6(1) GDPR.</u>

The continued storage of the complainant's personal data also constitutes a violation of Article 6 (1) GDPR. The permissibility of data processing follows the principle of prohibition with an exception. Accordingly, any data processing must satisfy both the principles set out in Article 5 GDPR and at least one of the legal grounds set out in Article 6(1)(a) to (f) GDPR. The continued storage of the complainant's personal data constitutes processing relevant under data protection law. A legal basis for the continued storage of the data after the request for erasure has been made is not apparent, as none of the conditions mentioned in Article 6(1)(a) to (f) GDPR apply.

You have the burden of proof for the existence of a permissible condition (Article 6(1), Article 5(1)(a) and (2) GDPR). You have not met this burden of proof, and according to the above explanations, there is no indication that a permissive circumstance existed.

As already explained, the complainant has in any case impliedly revoked any consent within the meaning of Article 6(1)(a) and Article 7(3) GDPR by

declaring his request for erasure, so that the continued storage of the complainant's personal data cannot be based on Article 6(1)(a) GDPR. Article 6(1)(b) GDPR is not a legal basis, as the complainant has terminated the customer relationship with [redacted] and further storage of his personal data was therefore no longer necessary. The continued storage cannot be based on Article 6(1)(f) GDPR either, as [redacted] has not proven the existence of legitimate interests in any case. Moreover, there is no necessity for the continued storage, so that Article 6(1)(c) to (e) GDPR cannot be considered as a legal basis either.

With regard to the e-mail stating that the e-mail address of the customer account had been changed, the facts of the case could not be clearly established.

III.
As a result, we decided not to take any further supervisory measures due to the violation, but to leave it at a reprimand.

The reprimand is based on Article 58(2)(b) GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after completing our investigation. We have again identified a violation on your part, which, however, was based in the past and should no longer occur as a result of the processes that have been changed in the meantime. You have comprehensively changed your processes and corrected the error immediately after it was identified.

In the certain expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Kind regards,

The Berlin DPA

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

521.11871
631.375
CR 52519

FINAL DECISION

Berlin, 21 June 2021

OUTFITTERY GmbH
Management Board
[redacted]
Leuschnerdamm 31
10999 Berlin

For information:
ISiCO Datenschutz GmbH
[redacted]
Am Hamburger Bahnhof 4
10557 Berlin

Reprimand
Complainant: [redacted]
Your letters of 15 January 2020, 30 June 2020, and 30 September 2020 (your reference IS-0472-10)

Dear [redacted],

We hereby issue a reprimand to your company for a violation of the General Data Protection Regulation (GDPR).

Reasoning:

This decision is based on the following considerations

I.
The Berlin DPA has established the following facts:

The above-mentioned complainant requested Outfittery GmbH to erase his data by email from the email address [redacted-email address 1] on 23 August 2019. Outfittery GmbH confirmed the erasure of the complainant's data by email on the same day.

On 23 September 2019, you sent the complainant an email to [redacted-email address 1] from team@modomoto.de with information about the merger of Curated Shopping GmbH with Outfittery GmbH, which was entered in the commercial register on 27 June 2019, and the transfer of his data to

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.

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/beschwerde.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

be Berlin

the system of Outfittery GmbH, unless he objects within two weeks of receipt of the notification.

By email from [redacted-email address 1] of 23 September 2019, the complainant requested an explanation from you and Curated Shopping GmbH as to why the erasure of his data had not taken place, objected to the further use of his data and again requested its erasure. Furthermore, the complainant stated that he had not had a business relationship with Curated Shopping GmbH.

In the above-mentioned statements, you credibly stated that the complainant had two customer accounts with Curated Shopping GmbH under the email addresses [redacted-email address 1] and [redacted-email address 2], independently of his customer account with Outfittery GmbH. You informed the complainant of this after receiving his renewed erasure request and confirmed to him in an email dated 26 September 2019 that you would also erase this data for his email address [redacted-email address 2].

II.

Legally, we assess the facts as follows. Your company has violated the General Data Protection Regulation (GDPR).

Pursuant to Article 17(1)(a) 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. The controller also shall have the obligation to erase personal data without undue delay if it is no longer necessary in relation to the purposes for which they were collected or otherwise processed.

According to Article 5(1)(a) GDPR, personal data shall be processed lawfully. In order for the processing to be lawful, personal data must be processed either with the consent of the data subject or on grounds of a legal basis, in accordance with Article 6(1) sentence 1 GDPR.

By email addressed to [redacted-email address 1], Curated Shopping GmbH with the email address team@modomoto.de informed the complainant on 23 September 2019 about the merger with Outfittery GmbH and the transfer of his data into the system of Outfittery GmbH, unless he objected within two weeks after receipt of the notification. However, this aforementioned email of 23 September 2019 is also attributable to Outfittery GmbH as the controller, since the merger with Curated Shopping GmbH was already entered in the commercial register on 27 June 2019.

Through his erasure request of 23 August 2019, the complainant has expressed that he is no longer interested in being contacted by Outfittery GmbH. Further storage of his data for the business purposes of Outfittery GmbH was thus no longer necessary. The erasure request was also not denied for other reasons.

However, an erasure did not take place with regard to the complainant's personal data taken over by Curated Shopping GmbH with effect from 27 June 2019 by Outfittery GmbH. Rather, his data was used again by Outfittery GmbH on 23 September 2019, although it should have already been erased. The use of the data and the continued storage thus took place without legal grounds.

Outfittery GmbH has thus violated Article 17(1), Article 5(1)(a) and Article 6(1) GDPR.

III.

As a result, we have decided not to take any further supervisory measures due to the violation, but to leave it at a reprimand.

The reprimand is based on Article 58(2)(b) GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after completing our investigation. We have again identified a violation on your part.

In the certain expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Kind regards,

[redacted]

Berlin Commissioner
for Data Protection
and Freedom of Information

631.119.2
A56 81640
CR 427592
DD 427633

09 September 2022

Final Decision

1. Core information on the Data breach

- Controller: Care.com Europe GmbH (provider of care services/household help)
- Incident: Unauthorized access to an email inbox of a senior employee with known access data.
- Time of incident: January 26 and 28, 2019.
- Time of awareness of the incident: January 28, 2019.
- EEA member states affected, each with number of data subjects there: See attachment for details
- Category of data subjects: Platform users, employees
- Category of data types/data sets concerned: Primarily (business) contact data; otherwise: Copy of ID (1 data subject in Romania), correspondence with police forces in UK and Germany due to police investigations (1 data subject in Germany, 2 data subjects in UK).
- Probable consequences of personal data breach: Misuse of the above data

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

Access to an e-mail box (online Outlook) of an employee with known access data. The origin of the access data could not be determined.

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Friedrichstr. 219, 10969 Berlin
Visitors' entrance: Puttkamerstr. 16-18

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

Office hours: Daily from 10 am to 3 pm, Thursdays from 10 am to 6 pm

Mail: mailbox@datenschutz-berlin.de
Web: www.datenschutz-berlin.de

BERLIN

3. Description and analysis of the effectiveness of the measures taken to remedy the data breach or mitigate any negative consequences
(Article 33 (3) d) GDPR)

The company has had the security leak comprehensively investigated, also by involving third parties. In this way, it was possible to limit the scope of unauthorized access to the online Outlook mailbox of an employee. The manipulations to the mailbox (e-mail forwarding) were reversed within 2 hours of the unauthorized access and access to the mailbox was blocked. In addition to resetting the data subject's password, 2-factor authentication was implemented for all employees.

The measures described above are sufficient to prevent unauthorized access in the future. Microsoft's Office online services also offer a sufficient level of IT security.

4. Notification of the data subjects or public announcement
(Article 34 para. 1 or Article 34 para. 3 lit. c) GDPR)

The 4 data subjects mentioned on point 1 (7th indent) were notified in writing. Apart from that, notification was not necessary (no high risk and see points 5 and 6 below).

5. Technical and organizational 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 for the data subjects is unlikely to persist (Article 34 (3) (b) GDPR)

Use of 2-factor authentication for all employees*.

7. Measures intended by the lead Berlin DPA.

Against the background of the above considerations regarding Article 33, 34 GDPR, the Berlin DPA proposes to discontinue the procedure and to close the case.

19 November 2021

Final Decision

Complaint against [redacted] – Right to rectification (Article 16 GDPR)

IMI Case: 62334
IMI A61VMN: 312886
IMI A60DD: 330086

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter "HBDI") refers to the complaint lodged by Mr. L. G. (hereinafter "Complainant") against [redacted] (hereinafter "[redacted]") with the French Data Protection Authority concerning the right to rectification.

1. Case Description

The Complainant, who was born on [redacted] 2001, created an account with [redacted] in 2014. In order to circumvent restrictions that would have been associated with a minor's account, he untruthfully stated [redacted] 1996 as his date of birth. As an account name, which he was free to choose, the Complainant chose the pseudonym "[redacted]", the name [redacted] being his mother's first name.

After the Complainant had reached the age of majority, he requested the correction of the account name and the date of birth stored by [redacted]. [redacted] refused both, which is why the Complainant lodged a complaint with the French DPA.

2. Investigation outcome

With regard to the account name, there is no entitlement to rectification. A pseudonym freely chosen by the data subject cannot be incorrect within the meaning of Article 16(1) GDPR, even if it may contain names or other data of third parties.

Regarding the rejected correction of the date of birth, [redacted] was asked by the HBDI to comment. [redacted] replied that the correction had been rejected by the customer support because the provision of a false date of birth when creating an account violates the user contract. Depending on the age of the account holder, [redacted] would provide different functions and services. In addition, the request and storage of the date of birth serves the fulfilment of legal obligations. Since a subsequent change of the date of birth can have far-reaching consequences, users cannot change it themselves. This is

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

also pointed out to users when they create an account. Requests to change the date of birth would be examined more closely by [redacted] with regard to possible consequences. After reviewing the facts, the Complainant's date of birth would now be changed and he would be informed accordingly. This case was also taken as an opportunity to review the processes in the customer support and to adjust the underlying work instructions.

3. Decision

In its Draft Decision of 07 October 2021, the HBDI has informed the supervisory authorities concerned that it intends to issue a warning to [redacted] pursuant to Article 58(2)(b) GDPR, as the correction of the Complainant's date of birth was initially improperly refused by [redacted]'s customer support. The right to rectification exists regardless of possible consequences under civil law in the contractual relationship between [redacted] and the Complainant. Accordingly, the processes in customer support must be adapted so that a correction is not generalized rejected in future, comparable cases. The HBDI found that further measures or sanctions are not necessary, as [redacted] has already initiated the rectification of the Complainant's date of birth as well as the adjustment of the work instructions on its own initiative. Moreover, the Complainant himself was responsible for the reason for the necessary correction by deliberately providing false information. No objections to the Draft Decision were raised by the supervisory authorities concerned.

The HBDI therefore issued a warning to [redacted] and concludes the proceedings with this Final Decision.

The Hessian DPA

[redacted]

Gustav-Stresemann-Ring 1 · 65189 Wiesbaden · Telephone +49 6 11 14 08 – 0 · Fax +49 06 11 14 08 – 9 00 (or – 9 01)
Email poststelle@datenschutz.hessen.de · Web www.datenschutz.hessen.de

The Hamburg Representative for Data protection and freedom of information

With postal delivery certificate

The Hamburg Commissioner for Data Protection and Freedom of Information
Ludwig-Erhard-Str. 22, 20459 Hamburg

Peppermynt GmbH
for the attention of Mr [redacted]
Schwanenvik 14
22087 Hamburg

Ludwig-Erhard-Str. 22, 7th floor
20459 Hamburg
Phone: 040 - 428 54 - 40 51
Fax: 040 - 428 54 - 40 00

Contact person: [redacted]

E-Mail:mailbox@datenschutz.hamburg.de

Ref: M1/1388/2021

Hamburg, 01.10.2021

Reprimand pursuant to Art. 58 (2) (b) GDPR

Dear Mr. [redacted],

Pursuant to Art. 58 (2) (b) of the General Data Protection Regulation (GDPR), I hereby issue the following

R E P R I M A N D

1. Peppermynt GmbH has infringed Article 12(3) and (4) of the GDPR by failing to provide information in accordance with Article 15(1) of the GDPR within one month and by the late provision being incomplete.
2. Peppermynt GmbH is hereby formally **reprimanded** pursuant to Art. 58 (2) (b) GDPR on the basis of the violations referred to under 1.
3. Peppermynt GmbH shall bear the costs of the proceedings. A separate decision will be issued on the amount of the costs.

After examination of the factual and legal situation, there is a processing operation that violates the GDPR. Pursuant to Article 58 (2) (b) of the GDPR, the controller may be reprimanded in the event of an infringement.

I. Facts

On 29.12.2020 as well as on 4.1.2021 the complainant Mr. [redacted] (hereinafter: Bf.) received one e-mail each from the sender address noreply@peppermynt.de, in which the products of Peppermynt GmbH "Wunder Box" and "Gold Oase" were advertised. The e-mails contained individualised links, including the phrase "why did I get this?“. The website called up via this gave the indication that the e-mail address was assigned to a "Peppermynt player".

On 21.1.21 the complainant sent a request for information pursuant to Art. 15 GDPR to Peppermynt GmbH by registered mail from Vienna. In this letter, the complainant requested information on which of his personal data Peppermynt GmbH was processing, information on the processing, whether a transfer to a third country was taking place and a copy of his personal data (Art. 15 (1)-(3) GDPR). Peppermynt GmbH did not reply to the complainant's letter.

On 26 February 2021, the complainant filed a data protection complaint with the Austrian data protection authority. The latter forwarded the complaint to the HmbBfDI on 10 March 2021.

By letter dated 18.5.2021, the HmbBfDI heard Peppermynt GmbH on the proceedings. In this letter, reference was made to the one-month period for the processing of data protection requests by data controllers under Article 12 (3) sentence 1 of the GDPR.

On 4 June 2021, the [redacted] of Peppermynt GmbH, [redacted], contacted the HmbBfDI on behalf of the company. He stated that Peppermynt GmbH, as a young company, had no experience in responding to data protection requests and asked for support. The HmbBfDI informed the complainant that the personal data processed would have to be made available.

In an e-mail dated 21.6.2021, Peppermynt GmbH informed the complainant that no "user" with the complainant's e-mail address existed and that accordingly no personal data of the complainant was stored.

Upon inquiry by the HmbBfDI with reference to the e-mails that the complainant had previously received, Peppermynt GmbH explained that the complainant's e-mail address had been included in Peppermynt GmbH's database due to an incorrect migration of the external service "Mailchimp", but had now been deleted. The complainant would not receive any further e-mails from Peppermynt GmbH in future.

II. Legal assessment

The prerequisites for a reprimand to be issued to Peppermynt GmbH pursuant to Art. 58 Para. 2 lit. b GDPR are met.

1. Infringement of Art. 12 (3) sentence 1 GDPR

There is an infringement of Article 12 (3) sentence 1 of the GDPR. According to the provision, information about requests pursuant to Art. 15-22 of the GDPR must be provided without delay, but in any case within one month. Peppermynt GmbH did not respond to the complainant's request pursuant to Art. 15 of the GDPR within one month.

2. Infringement of Article 15(1) of the GDPR

There is an infringement of Article 15 (1) of the GDPR. According to the provision, data subjects have the right to request information about their personal data processed. The controller must provide this or provide negative information. [1] It is therefore not up to the data subjects to communicate in which system of the controller the data might be stored.

In its information, Peppermynt GmbH informed the complainant that it did not process any of his personal data. In deviation from this information, Peppermynt GmbH had, however, stored the complainant's email address-. The email address is personal data in the sense of Art. 4 No. 1 GDPR. The e-mail address is information which refers to the complainant as an identified person. The negative information was therefore issued incorrectly.

3. Decision-making and discretion

There are infringements of the GDPR, so that corrective powers pursuant to Art. 58 (2) GDPR are to be taken. There are no reasons not to make use of these. This is the first finding by the HmbBfDI that Peppermynt GmbH has violated the GDPR, so that the reprimand is to be chosen as the mildest possible means.

With kind regards

[redacted]

Remedies:

An action against this decision may be brought before the Hamburg Administrative Court (Lübeckertordamm 4, 20099 Hamburg) within one month of notification.

---

[1] *Franck*, in: Gola, Datenschutz-Grundverordnung, 2nd ed. 2018, Art. 15 Rn. 5.

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

631.106.4
CR 66495

8 November 2021

Final Decision pursuant to article 60 (8) GDPR

Preliminary comments

In July 2018 the Berlin DPA received a complaint (reference number 521.10011 / 631.106) about the controller Spotify regarding the use of cookies on Spotify´s homepage. A procedure pursuant to article 56 was started in the IMI, in which Sweden resulted as Lead Supervisory Authority.

In November 2020, the Swedish Supervisory Authority IMY broadcasted a Draft Decision (DD 164968) to close the case because "in Sweden the use of cookies is regulated in the Privacy and Electronic Communications Directive which is incorporated into the Swedish Law through the Swedish Electronics Communications Act (ECA), over which The Swedish Post and Telecom Authority (PTS) is the supervisory authority". The Draft Decision received a series of comments asking for clarification but no formal objection.

In October 2021, it was clarified between the Berlin DPA and the Swedish Supervisory Authority that the aforementioned Draft Decision had been intended as a decision pursuant to article 60 (8) GDPR.

For this reason, an in order to comply with article 60 (8) GDPR and close the case, the Berlin DPA hereby adopts the Draft Decision 164968 as it was originally formulated by the Swedish Supervisory Authority:

> "**Complaint concerning Spotify's privacy policy**
>
> **Regarding the complaint against Spotify in IMI case register (66495).**
>
> **Background**
>
> The complainant alleged that in order to access information on Spotify's website one have to activate cookies. Spotify also wants to force the user to accept cookies, although this should be optional. It is stated on the website that the consent to cookies can be modified or withdrawn. That is however false according to the complainant since the service doesn't work without the use of cookies.
>
> **Finding**

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.

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/beschwerde.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

The Swedish Data Protection Authority has received several complaints after GDPR came into force concerning websites that allegedly use cookies and other tracking technologies non-compliantly with applicable law.
Unfortunately, we can neither inspect, review nor influence the use of such technologies. The information provided in this complaint will therefore not lead to any further actions by the Swedish SA.

The following background information and legal grounds are applicable. In Sweden the use of cookies is regulated in the Privacy and Electronic Communications Directive which is incorporated into the Swedish Law through the Swedish Electronics Communications Act (ECA), over which The Swedish Post and Telecom Authority (PTS) is the supervisory authority.

After having assessed the circumstances in the now relevant case we have concluded that the complaint mainly concerns the collection of and consents to the use of cookies. The competent authority to initiate an audit toinvestigate the subject matter is the Swedish Post and Telecom Authority.

With this informational letter the case will hereby be closed.”

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 16 November 2021

535.2907 / 631.447

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.

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/beschwerde.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

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** Delivery Hero SE
- **Incident**: Due to a manual configuration error at the food delivery service Delivery Hero, stored photos of rejected orders were publicly accessible; on 19,000 photos, the invoice was also displayed. In about 400 of the photos with invoices, the name and telephone number of the person placing the order were also visible. A breakdown by country was not provided.
- **Date of occurrence**: 4 March 2021 – 20 July 2021
- **Date of acknowledgement of the incident**: 20 July 2021
- **EU/EEA Member States concerned, with the number of data subjects concerned**: Bulgaria, Croatia, Cyprus, Czech Republic, Finland, Greece, Hungary, Norway, Sweden, Romania
- **Category of data subjects**: Customers
- **Category of the data types/data records concerned**: Pictures of delivered dishes, partly with customer data (name, phone number, NO delivery addresses)
- **Likely consequences of the violation of the protection of personal data**: Probably little or no consequences, as no unusual accesses and especially no accesses on a large scale to the cloud storage were detected. In addition, only relatively uncritical personal data was affected, in the majority even only images without any personal reference. Possible consequences: Identity theft, unwanted calls

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

Due to a manual configuration error, between 4.3.2021 and 20.7.2021, 170,000 photos of rejected orders stored in a cloud bucket were publicly accessible, on 19,000 of which the receipt was also shown. About 2% of the photos with receipts also showed the name and telephone number of the person placing the order. There are therefore about 400 data subjects. There was no breakdown by country. Retrieving the photos also required knowledge and manipulation of the corresponding URLs.

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)

be Berlin

- Erasure of the cloud bucket, moving the data to a storage that cannot be accessed without authentication.
- Checking all other buckets for faulty configuration
- 4-eyes principle for the configuration of access rights has been implemented
- Automated analysis of the photos to see whether the photos contain a receipt and whether personal data can be read on the receipt.
- In the future, the company will draw customers' attention to the fact that such receipts should not contain any personal data when using the app function for uploading pictures.

We consider the measures to be sufficient and effective.

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

Notification of the data subjects is not mandatory, as there is no high risk due to the non-critical data and it is unlikely that unauthorised access to personal data has occurred.

No read logging was (inadvertently) set up on the bucket (cloud storage area), so no object-level analysis is possible. However, coarser data traffic analyses did not show any anomalies such as large-scale data retrievals.

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

For services and other storage, automated erasure rules generally apply for erasure after 6 months. In the present case, however, this functionality had not been activated by mistake.

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 point 3.

7. Intended measures by the LSA Berlin DPA

In the light of the above-mentioned considerations, the Berlin DPA closes the case.

Baden-Württemberg
THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 ·D-70025 Stuttgart

[redacted]
[…]

File No. R 2482/249

Supervisory data protection investigation in accordance with Article 57(1)(a), (f) and Article 58(1)(b) GDPR
[redacted] – Your Ref. no. […]
Your letter of 28 June 2021

Dear Madam or Sir,

Having examined the facts of the case we get back to you regarding the complaint under the above-mentioned Ref. no.

I. The course of the procedure

The Baden-Wuerttemberg DPA (hereinafter: BW DPA) launched an investigation based on the complaint of [redacted] (hereinafter: the Complainant) pursuant to Article 57(1)(f) of the General Data Protection Regulation (hereinafter: GDPR).

In July 2018, the Complainant lodged a complaint with the Data Protection Authority of Austria, in which he presented that he had exercised his right of access as per Article 15 GDPR to [redacted], [redacted] (hereinafter: Controller). According to his allegations, he has received no response within a month.

The Austrian DPA submitted the complaint to our DPA (DE/BW) in August 2018 via an Article 56 procedure in IMI (no. 48007). The DE/BW DPA agreed to handle the case as LSA and created a case register in IMI (no. 71144).

After concluding the investigations, the draft decision was shared preliminary with the CSAs in A60IC 429634. Only the AT DPA raised some questions which we could answer to their full satisfaction (61VMN 507475). We did not receive comments from one of the other CSAs.

Subsequently, the draft decision was formally shared as per Article 60(3) GDPR with the CSAs in A60DD 507994. There were no comments or objections raised to the draft by any of the CSAs.

II. Facts of the case

The complainant states that he had sent an access request to the controller on 3 June 2018 via the website contact form [redacted]). Even though the receipt had been confirmed, the request had not been dealt with within one month. He claims that by the time the complaint was filed, he had received no response.

The DE/BW DPA contacted the Controller in order to ask them for a response to the facts the complainant presented. We also forwarded the access request to the Controller, which the complainant had enclosed to the complaint. There was an exchange of different correspondence with the Controller in the following months.

On 29 June 2021, a law firm informed the DE/BW DPA that they would legally represent the Controller in the proceeding. They submitted a comprehensive statement regarding the complainant's allegations in which they state that the accusation that their client would not have answered the access request of the complainant is not true, but that, based on the data protection regulations in force at the time, the information request was fully answered by letter of 13 July 2018. However, after such a long time, ascertaining that the complainant received the letter, would no longer be possible due to the fact that certificates of delivery held by the German post office are only valid for one year. The letter sent to the complainant on 13 July 2018 does not show a date of receipt. They also state that in 2018 it was standard practice of their client to always grant such access requests by mail.

The client was therefore surprised to learn from the correspondence that the complainant did not receive the information letter. They immediately provided the requested information and sent it to the Complainant again on 28 June 2021, together with evidence about the respective business relationship as regards the purchases made by the complainant, in accordance with the applicable processes currently in force.

III. The findings of the Authority

Pursuant to Article 12(1) 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. According to 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, whereby that period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

Based on the statement and documents submitted by the Controller, it is evident for the DE/BW DPA that they have complied with the complainant's access request as per Article 15 GDPR already on 13 July 2018, as the copy of the letter sent to the complainant is still in the possession of the Controller and shows this date. The fact that the postal receipt is no longer valid is not a fact the controller could have any influence on. At the latest, the information has been delivered to the complainant subsequently after the DE/BW DPA conducted the investigation.

Nevertheless, also sending the information to the complainant already on 13 July 2018 would have been outside of the one-month deadline of receipt of the request as per Article 12(3) GDPR.

It is not apparent that the Company was in a situation of Article 12(2) or (3) GDPR. Firstly, the Company was able to identify the Complainant, meaning that there was no reason for asking for further identification of the Complainant. Secondly, the Company has not indicated that they process such a wide scope and large number of data so as to request the Complainant to specify his request.

Additionally, the Controller did not inform the data subject within a month about not taking action on the request together with reasons for not taking action as requested by Article 12(4) GDPR.

By not having reacted to the Complainant's access request without undue delay, they have **infringed Article 15(1) as well as Article 12(1) and (3) GDPR**.

IV. Legal consequences

The DE/BW DPA establishes that the Company breached Article 15(1) as well as Article 12(1) and (3) of the GDPR, as the Complainant's access request has not been dealt with in due time.

However, due to the constellation explained, the controller was in the situation to validly believe to have answered the access request of the complainant. They apologised for this mistake and immediately provided the requested information to the Complainant (again).

In addition, the Company has been very cooperative during the regulatory and supervising process. Following the investigation of the DE/BW DPA, the Controller immediately gave the requested information.

Hence, the BW DPA issues a **reprimand** to the company for the abovementioned infringements of the GDPR, based on Article 58(2)(b) GDPR.

We will also reiterate to the Controller again the fact that requests under Articles 15-22 GDPR must be answered without undue delay, at the latest within one month, and that the Controller must implement internal processes that ensure a response within this deadline.

V. Information on legal remedies

An appeal against this decision may be filed in writing, electronically or for recording with the Administrative Court of Stuttgart, Augustenstraße 5, 70178 Stuttgart, within one month of notification pursuant to Article 78 of the General Data Protection Regulation in conjunction with Section 20(1) and (3) of the Federal Data Protection Act.

LDA Brandenburg - Stahnsdorfer Damm 77 - 14532 Kleinmachnow

[redacted]

[redacted]

Date:	10 November 2021
Processors:	[redacted]
Phone:	[redacted]
Fax:	[redacted]
Reference:	Mi/ 154/20/0192
IMI:	A60 DD 314880

(Please indicate characters when replying)

Insufficient implementation of technical and organisational measures when operating a web shop - warning pursuant to Art. 58 para. 2 letter b of the General Data Protection Regulation (GDPR)[1]

- Data breach notification on 30 January 2020 and the following correspondence
- last: our hearing on the warning of 14 September 2021

Dear [redacted]

in the above-mentioned matter, the following is issued against [redacted] represented by [redacted] and [redacted]

Notice:

It is established that [redacted] represented by [redacted] and [redacted] has violated Article 25(1) and Article 32(1)(b) of the GDPR in relation to the upload function for image files which was not sufficiently secured by technical and organisational measures, the customer data shop which was not sufficiently protected and the outflow of personal data from the company's web shop in connection with the data protection breach of 26 January 2020.

Due to this infringement, [redacted] represented by [redacted] and [redacted] is warned in accordance with Article 58(2)(b) of the GDPR.

[1] General Data Protection Regulation of 27 April 2016 (OJ EU L 119, 4 May 2016, p. 1; L 127, 23 May 2018, p. 2; L 74, 4 March 2021, p. 35).

Justification:

I.

[redacted] perates a web shop for mobile phone accessories at the addresses [redacted] Customers can buy cases, protective foils, cables, adapters, batteries, chargers, headphones, etc. for mobile phones and tablets. In addition, [redacted] offers its customers the opportunity to design the cases themselves. For this purpose, they can, among other things, upload personal image files to the web shop's internet platform, edit them there and have them printed on (blank) mobile phone cases. For the operation of the web shop [redacted] uses [redacted] based in Poznań (Poland) as a processor.

On 30 January 2020, [redacted] nformed my authority in the context of a data breach notification pursuant to Article 33 of the GDPR that the IT systems of its processor [redacted] were compromised on 26 January 2020. In the process, the customer database of [redacted] was also stolen. In a message sent to [redacted] on 28 January 2020, the attacker(s) threatened to publish the customer data as well as further unauthorised activities on the web shop's platform if a certain amount of money was not paid by 31 January 2020.

[redacted] nformed not only the competent data protection supervisory authority about the incident, but also the customers in accordance with Art. 34 DS-GVO. Subsequently, on 16 February 2020, a data subject filed a complaint against [redacted] with my authority pursuant to Art. 77 DS-GVO, complaining about the company's breach of data protection regulations, in particular the lack of technical and organisational measures.

In order to clarify the facts and to determine the causes of the data breach, my authority contacted [redacted] ithin the framework of hearings on 2 March, 22 April, 20 July and 24 September 2020 with the request to provide the necessary information. The company's statements were dated 23 March, 30 April, 17 August and 14 October 2020 and 8 January 2021 respectively. In the context of the clarification of the facts, it was particularly important to find out how the attack proceeded in detail, which technical and organisational measures the company and the processor had implemented prior to the incident, why these measures were not fully effective and which supplementary measures were necessary to ensure technical data protection and information security or were implemented after the incident.

After evaluating the company's comments, the following emerges:

- According to [redacted] the data protection breach was triggered by a manipulated image file in JPG format, which the attacker(s) had uploaded to the web shop's platform using the function to design their own mobile phone cases. The image file contained hidden commands (script code in the programming language PHP), the execution of which made it possible to read out the customer database of [redacted] The message subsequently sent by the attacker(s) to [redacted] s order processor shows that it would also have been possible to execute other malicious functions (e.g. manipulating database entries or deleting the entire database).

- [redacted] further announced that 76,797 customers from Germany and Austria were probably affected by the incident, including 9,862 people who had created a customer account via the [redacted] site since 19 May 2017. Further people from other EU countries were also affected, including Poland, the Czech Republic, Slovakia and Hungary. In total,

up to 725,697 database entries were expected. The categories of personal data stored in the customer database in question included surname, first name, address, telephone number, e-mail address, user name and password, and, in the case of commercial customers, company name and tax number, insofar as they related to an identifiable natural person.

- The technical basis of the web shop is the open source version (Community Edition) of the product "Magento". At the time of the data protection breach, version 1.9.3.2 was used; during the investigation, version 1.9.4.4 was updated.

- According to [redacted] a number of security measures were implemented in the web shop before the incident. In addition to the standard mechanisms of the "Magento" product, these included authentication of access to servers based on asynchronous cryptographic procedures (via SSH key pairs), logging of all server activities and regular updates to close security gaps.

- As a consequence of the incident, the entire IT system of the web shop was thoroughly checked and a number of additional security measures were implemented. These include the exchange of SSH keys for authorised access, monitoring relevant system files for changes in access keys, checking the system's open ports, checking all system and home directories for malware and unwanted files and deleting them if necessary, and blocking the execution of PHP scripts from certain directories.

In the course of processing the file, [redacted] submitted a list of processing activities pursuant to Article 30 of the GDPR and a processing contract pursuant to Article 28 of the GDPR with [redacted]

In a letter dated 14 September 2021, my authority announced to [redacted] that it would issue a warning for violations of the General Data Protection Regulation pursuant to Article 58(2)(b) of the GDPR. The company did not take the opportunity to comment.

II.

My authority is responsible for monitoring data protection regulations vis-à-vis non-public bodies in the State of Brandenburg in accordance with Article 51 (1) of the Data Protection Regulation in conjunction with Section 40 (1) of the Federal Data Protection Act (BDSG) [2][3]and Section 18 (3) of the Brandenburg Data Protection Act (BbgDSG) and [4]locally in accordance with Section 3 of the Administrative Procedure Act (VwVfG) [5]in conjunction with Section 1 (1) of the Administrative Procedure Act for the State of Brandenburg (VwVfGBbg). [redacted] represented by [redacted] and [redacted] as a legal entity with its registered office in the State of Brandenburg, is a non-public body in the sense of § 1 para. 1 sentence 2, § 2 para. 4 sentence 1 BDSG, which is subject to my supervision.

---

2 Act on the Protection of Personal Data in the State of Brandenburg of 8 May 2018 (GVBl. I/18, [No. 7]) amended by Article 7 of the Act of 19 June 2019 (GVBl. I/19, [No. 43], p. 38).

3 Federal Data Protection Act of 30 June 2017 (BGBl. I p. 2097), as amended by Article 10 of the Act of 23 June 2021 (BGBl. I p. 1858).

4 Administrative Procedure Act for the State of Brandenburg of 7 July 2009 (GVBl. I/09, [No. 12], pp. 262, 264), last amended by Article 6 of the Act of 8 May 2018 (GVBl. I/18, [No. 8], p. 4).

5 Administrative Procedure Act (Verwaltungsverfahrensgesetz) in the version promulgated on 23 January 2003 (BGBl. I p. 102), as last amended by Article 24(3) of the Act of 25 June 2021 (BGBl. I p. 2154).

The legal basis for the warning is Article 58(2)(b) of the GDPR. According to this, the supervisory authority is allowed to warn a controller if it has violated this regulation with processing operations.

The hearing requirement of Section 28 VwVfG in conjunction with Section 1 (1) VwVfGBbg prior to the issuance of an onerous administrative act was taken into account, as my authority gave you the opportunity to comment on the announcement to issue a warning pursuant to Article 58 (2) (b) of the GDPR in the hearing letter of 14 September 2021. You did not make use of the opportunity to comment within the set deadline.

As part of the cooperation pursuant to Article 60 of the GDPR, my authority, as the lead data protection supervisory authority, sent the necessary information and the draft decision with the announcement that a warning would be issued against [redacted] to the other European data protection supervisory authorities concerned for their comments. No relevant and substantiated objections to the draft decision within the meaning of Article 60 (4) of the GDPR were subsequently received.

In the web shop at the above-mentioned internet addresses, [redacted] processes personal data within the meaning of Art. 4 No. 1 DS-GVO. The information collected from the customers of the shop, such as surname, first name, address, contact details, etc., are data of concrete natural persons which serve to identify these persons or enable third parties to do so. The handling of this data by [redacted] includes, among other things, the collection, storage, use, modification and deletion of the data and thus processing operations covered by the definition in Art. 4 No. 2 DS-GVO.

After evaluating the information provided by [redacted] during the above-mentioned hearings on the data protection incident on 26 January 2020, as well as the documents submitted, I have identified violations of the following data protection regulations:

a) Infringement of Article 25(1) and Article 32(1)(b) of the GDPR due to the insufficient protection of the web shop against the uploading of executable code with malicious functions.

Pursuant to Art. 25 para. 1 DS-GVO, the controller (here: [redacted] shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons represented by the processing, implement appropriate technical and organisational measures, both at the time of the determination of the means for the processing and at the time of the processing itself, which are designed to implement the data protection principles effectively and to incorporate the necessary safeguards into the processing in order to meet the requirements of the GDPR and to protect the rights of data subjects.

According to Article 5(1)(f) of the GDPR, the data protection principles include, in particular, that personal data are processed in a manner that ensures appropriate security of such data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage ("integrity and confidentiality").

Article 32 (1) of the GDPR specifies the requirements in such a way that the controller and the processor must take appropriate technical and organisational measures to ensure a level of

protection appropriate to the risk. Pursuant to letter b of the said provision, these measures include measures to ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing on a permanent basis. According to Article 32(2) of the GDPR, the assessment of the adequate level of protection shall take into account, in particular, the risks associated with the processing, specifically the risks of destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

[redacted] offered the customers of its web shop to upload personal files (e.g. image files) to the internet platform operated by [redacted] for the design of mobile phone cases (upload of files). This offer is not objectionable from a data protection perspective. However, [redacted] should have carefully and in detail assessed the risk of misuse of the upload function at the time the service was designed. In the event of an existing, not insignificant risk to the rights and freedoms of the data subjects, it should have planned suitable and appropriate technical and organisational measures to mitigate the risk. This follows from Article 25(1) of the GDPR ("at the time of determining the means of processing").

Furthermore, it follows from the same provision as well as from Article 32 (1) (b) of the GDPR that [redacted] should also have implemented the corresponding technical and organisational measures within the internet platform it offers ("at the time of the actual processing"), in particular to permanently ensure the confidentiality and integrity of the systems and services. In this way, it would have been possible to prevent in a timely and effective manner any unauthorised modification of the system or the services offered through the infiltration and execution of malware and thus a violation of the integrity of the system or the services. The same applies with regard to the prevention of unauthorised access to the personal data stored in the customer database for attackers and thus the prevention of a breach of the confidentiality of the processing.

In the present case, [redacted] either did not assess the risks of compromising the web shop's internet platform by uploading malware via the upload function offered, or assessed these risks as too low and thus incorrect. As a result, [redacted] failed to plan and implement sufficient technical and organisational measures that could have counteracted a compromise.

When assessing a risk to the processing of personal data, both the probability of occurrence and the amount of potential damage must regularly be considered (cf. Art. 25(1) DS-GVO and Art. 32(1) DS-GVO). [redacted] should have been aware that the offer to upload files to the internet platform it operates also attracts attackers who attempt to place software with malicious functions there and execute it in the context of processing personal data. The likelihood of such misuse activities is significant, as confirmed by frequent reports of such security incidents on internet platforms as well as recommendations for countermeasures.[6] The amount of the potential damage was also underestimated by [redacted] After all, more than 76,000 customers of the company were affected by the incident in question here in Germany and Austria alone; according to [redacted]s own information, a total of more than 725,000 customer-related data records could have been read by attackers and used for criminal activities (such as identity theft or phishing).

---

[6] see messages on relevant portals, such as "Attackers could upload malicious code to millions of WordPress websites" (https://heise.de/-4993717), "Infected add-ons found on Mozilla download page" (https://heise.de/-923719), "Google Drive vulnerability makes it easy to infiltrate malware" (https://winfuture.de/news,117795.html), "Protecting against file upload risks" (https://www.all-about-security.de/allgemein/schutz-gegen-die-risiken-bei-datei-uploads/), last accessed on 1 November 2021 in each case.

Since compromising internet platforms by uploading and executing malware is one of the greatest risks in web applications, it is also considered in important standard publications on information security. Examples include the IT-Grundschutzkompendium of the German Federal Office for Information Security[7] (BSI), the handout "State of the Art" of the Bundesverband IT-Sicherheit e. V. (TeleTrust), or the German Federal Association for IT Security (Bundesverband IT-Sicherheit e. V.). [8](TeleTrust) or the documents of the Open Web Application Security Project [9](OWASP). These publications also contain recommendations for effective and suitable countermeasures that help prevent the compromising of an internet platform (such as a web shop) through the infiltration and execution of malware.

For example, the IT-Grundschutzkompendium of the BSI (version 2020) lists in the module APP. 3.1 "Web applications", for example, lists the threats G 0.23 - Unauthorised intrusion into IT systems, G 0.36 - Identity theft and G 0.39 - Malware. The countermeasures discussed in this module include, for example, the mandatory measures APP.3.1.A4 - Controlled inclusion of data and content in web applications, APP.3.1.A16 - Comprehensive input validation and output encoding, and the recommended measure APP.3.1.A22 - Checking web applications for security vulnerabilities. Also the module APP. 3.2 "Web server" of the IT-Grundschutzkompendium also lists G 0.23 and G 0.39 among the threats. The countermeasures include the mandatory measure APP.3.2.A3 - Securing file uploads and downloads and the recommended measure APP.3.2.A14 - Integrity checks and protection against malware. By implementing the aforementioned measures, [redacted] could have effectively prevented the attacker(s) from uploading malware in a manipulated image file to the company's internet platform and executing it there.

Nothing else emerges when the other sources mentioned above are consulted. The handout "State of the Art" of the German Federal Association for IT Security (Bundesverband IT-Sicherheit e. V.). (as of 2021) lists in chapter 3.2.19 "Protection of web applications", among other things, "command injection" - i.e. the introduction of executable malicious code into the application - as a significant threat. As a protective measure, the use of a web application firewall to examine and block potentially harmful data traffic (here: during upload) is recommended.

Furthermore, the Open Web Application Security Project (OWASP) has listed "injection" among the top 10 security risks in web applications for several years - currently (2021) in third place (A03), in the previous edition (2017) in first place (A01). Injection" refers to risks from unvalidated, unfiltered or untreated data provided by users (or attackers). Several Common Weaknesses contribute to the high ranking of the risk, including CWE-77 Command Injection, CWE-94 Code Injection and CWE-96 Static Code Injection. The above descriptions also include recommended countermeasures, in particular input validation. In addition, the test for uploading malicious files is part of the Web Security Testing Guide of the OWASP (point 4.10.9 there), and should therefore be carried out regularly before commissioning and during operation when carefully testing web applications.

The measures listed in the publications mentioned as "mandatory" or "recommended" for the operation of web applications are to be qualified as state of the art. They have been developed from the abstraction of frequent security incidents and countermeasures of responsible persons and have proven themselves in practice. The implementation of the measures by [redacted] would not only have been suitable and appropriate to prevent the data protection breach in

---

7 see https://www.bsi.bund.de
8 see https://www.teletrust.de
9 see https://www.owasp.org

question. It was also necessary to control the risks for data subjects associated with data processing. With regard to the implementation costs, it can be assumed that the effort would have been reasonable and limited. This is already shown by the short-term action of the company, which already stated in the notification of 30 January 2020 that it would now block the execution of PHP code from certain directories of the file system and thus ensure the integrity of the processing of personal data.

b) Infringement of Art. 25(1) and Art. 32(1)(b) of the GDPR due to insufficient protection of the web shop against unauthorised reading of the customer database.

According to the legal provisions cited above under II a), the controller and the processor are obliged to ensure not only the integrity of the systems and services for processing personal data, but also their confidentiality. This means that personal data must not be disclosed to unauthorised persons or come to their knowledge. As explained above, the technical and organisational protection measures shall be determined and implemented taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons represented by the processing.

The inadequate protection of [redacted] s web shop against the uploading and execution of malicious software also favoured the leakage of the customer database by the attacker(s). However, this part of the data protection breach could have been effectively prevented by appropriate technical measures separately and independently of the uploading of the malware. It must be noted that the company had neither designed appropriate measures at the time of the decision on the means of data processing nor implemented them at the time of the actual processing. Both constitute a violation of the above-mentioned regulations.

For insufficient analysis and evaluation of the risks emanating from the processing of personal data in the [redacted] web shop, their probability of occurrence and the amount of potential damages, please refer to II a).

As above, important information on risks and suitable protective measures according to the state of the art to prevent unauthorised access to personal data can be found in the literature. For example, the IT-Grundschutzkompendium of the BSI (as of 2020) lists the hazards G 0.19 - disclosure of information worthy of protection and G 0.36 - identity theft in module APP.3.1 "Web applications". Among the measures to be taken against the exploitation of these threats, APP.3.1.A2 - Access Control for Web Applications, which restricts users' access to data by means of restrictive permissions, is mandatory. Also to be mentioned is the module APP. 3.2 "Web server" with the obligatory measure APP.3.2.A2- Protection of web server files, which protects confidential data from unauthorised access and also counteracts the G 0.19 threat. The IT-Grundschutzkompendium also provides security measures for the network level, here in the module NET.3.2 "Firewall" for example the compulsory measure NET.3.2.A2 - Defining the firewall rules. Suitable rules must be used to prevent unauthorised connections from the protected network (e.g. connections to attackers for the purpose of data leakage) and data loss (vulnerability G 0.45).

In its publication "State of the art" in chapter 3.2.21 "Server hardening", the Bundesverband IT-Sicherheit e. V. (German Federal Association for IT Security) also recommends a restrictive con-

figuration of authorisations, restrictions in network settings and a corresponding configuration of the firewall to prevent data outflows from databases.

With regard to the Open Web Application Security Project (OWASP), it should be noted that the risk "Broken Access Control", which also includes the unauthorised leaking of information from web applications, is currently ranked number 1 of the top 10 risks. In the previous list from 2017, this risk was ranked 5th. The assigned common weaknesses are, for example, CWE-200 - Exposure of Sensitive Information to an Unauthorised Actor or CWE-402 - Transmission of Private Resources into a New Sphere (Resource Leak).

According to all of this, [redacted] should have been aware that there is a significant risk of customer data being leaked to unauthorised persons when operating the web shop. In particular, the company should have taken protective measures against the unauthorised establishment of a communication connection from the web application to the attacker and the mass leakage of this data, also independently of the measures to protect against the upload of malicious code to the platform. That these measures are state of the art is evident from the best practice recommendations cited above. Their implementation would also have been possible with a reasonable amount of effort. In particular, restricting the possible connection to the firewall and limiting the amount of data transferred from a database could have effectively prevented the data protection breach in the present case.

Due to the aforementioned violations, [redacted] represented by [redacted] and [redacted] is warned pursuant to Article 58 (2) (b) of the GDPR. The warning serves the purpose of bindingly establishing a violation of the legal provisions of the General Data Protection Regulation that has already occurred.

The warning proves to be proportionate in the individual case. It is suitable and necessary in order to make [redacted], represented by [redacted] and [redacted] aware of the infringement and to make them aware of the provisions of data protection law. In order to achieve this purpose, the supervisory authority does not have a milder means at its disposal which would be equally suitable. The warning does not create an immediate obligation to act and is not linked to the initiation of administrative offence proceedings or a fine. Therefore, it is usually used for simple violations that have not led to a significant threat to the fundamental right to data protection.

From the fact that [redacted] represented by [redacted] and [redacted] has not experienced any comparable data protection incident so far and that a high degree of cooperation prevailed during the clarification of the facts as well as during the initiation of necessary measures, I conclude that there is no reason for further remedial measures within the meaning of Article 58 (2) of the GDPR. The complaint of the data subject was also subsequently remedied in this respect.

The warning is also appropriate, i.e. proportionate in the narrower sense. In the required weighing of the conflicting interests, it must again be noted that the intensity of the intervention of the supervisory authority's measure is to be classified as rather low, whereas on the other hand a violation of data protection principles is established. The interest of [redacted] represented by [redacted] and [redacted] to be able to operate its business free of state interference must therefore take a back seat to the interest of the general public to

prosecute a violation of the right to data protection as well as the right to informational self-determination within the framework of the legal provisions.

Remedies:

An action against this decision may be brought before the Potsdam Administrative Court, Friedrich-Ebert-Straße 32, 14469 Potsdam, within one month of notification.

With kind regards

[redacted]

IMI Reference No. 429871

National Reference Number: [redacted]

In the matter of a complaint, lodged by [redacted], Poland with the Hamburg Commissioner for Data Protection and Freedom of Information pursuant to Article 77 of the General Data Protection Regulation, concerning [redacted]

FINAL DECISION SUI GENERIS FOR THE PURPOSE OF INTERNAL EDPB DOCUMENT 06/2021 ON THE PRACTICAL IMPLEMENTATION OF AMICABLE SETTLEMENTS, ADOPTED 18 NOVEMBER 2021

Hamburg, 2. February 2022

Background

On 5 November 2021, [redacted] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Hamburg Commissioner for Data Protection and Freedom of Information ("the **HmbBfDI**") concerning [redacted] ("the **Controller**"). As the Controller is based in Hamburg, Germany, the lead supervisory authority is the HmbBfDI in accordance with Art. 56 (1) GDPR.

The Complaint

1. The details of the complaint were as follows:

    a. The Data Subject is CEO of a public limited company, sp. z o.o.. In the Polish company's register entry of February 2019, the Data Subject's name is specified with a middle name initial "[redacted]". In February 2020, the Data Subject's name was changed from "[redacted]" to "[redacted]" in a register entry. In the next register entry dating February 2020, the Data Subject's name is shown without a middle initial.

    b. The Controller reproduces commercial register information in an online-database. The information regarding the Data Subject's name was published in graphic overviews including the middle initial "[redacted]."

c. The Data Subject emailed the Controller on 15 October 2021 to request deletion of the middle initial in its overview under URL [redacted]. The Controller stated that the middle initial had been contained in the company's register and demanded an official name certificate from the Data Subject to prove it has no such middle name. The Data Subject was of the opinion it had no obligation to provide an official name certificate.

Action taken by the HmbBfDI

1. The HmbBfDI started an Informal Consultation with PL SA (Office for the Protection of Personal Data) (IMI Reference No. 388073) in February 2022 as the Data Subject is residing in Poland. The HmbBfDI considered the concerns raised by PL SA in the consultation.

2. The HmbBfDI, having regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 ("**Document 06/2021**"), and considered that there is a reasonable likelihood of an amicable settlement being concluded between the parties within a reasonable time, and considered that (paragraph 64): only one data subject was affected, a systemic failure was not recognisable, there was an incidental or accidental data protection violation, as the middle name initial is contained in former company's register's entries, with the middle initial, a limited number of personal data was affected, the effects of the violation were not of serious nature and there is a small likelihood of further violations in the future.

Amicable Settlement

3. The HmbBfDI engaged with both the Data Subject and the Controller in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Controller was willing to change the name upon receipt of an official name certificate, but that the Data Subject was not willing to provide same.

4. In the circumstances, the Controller agreed to take the following action:

   The Controller agreed to delete the middle name initial from all of its graphic overviews, i.e. under URLs [redacted], [redacted] as well as [redacted] and [redacted] and in any URLs linked on its websites even without being provided an official name certificate by the Data Subject.

5. With this, the Controller has fully complied with the Data Subject's request to delete the middle name initial from the graphic overview under URL [redacted] as it has deleted the middle initial from its overviews on all of its websites accessible via the online-database.

6. On 29 June 2022, the Data Subject was provided with the Controller's answer that the middle name initial had been deleted from its graphic overviews and depictions of commercial register entries. The correspondence noted that the deletion by the Controller appeared to constitute the resolution of the Data Subject's complaint. The Data Subject did not provide any additional comments. The HmbBfDI did not receive any further communication from the Data Subject. Accordingly, as the Controller has fully complied with the Data Subject's request to delete the middle name initials from its database-websites, without being provided an official name certificate/identity card, the complaint has been deemed to have been amicably settled.

7. In circumstances where the subject-matter of the complaint has been amicably settled, in full, the complainant, in accordance with Internal EDPB Document 06/2021 on the practical implementation of amicable settlements (adopted on 18 November 2021), is to be informed of the consequences of the amicable settlement.

Confirmation of Outcome

8. For the purpose of Document 06/2021, the HmbBfDI confirms that:

    a. The complaint, in its entirety, has been amicably resolved between the parties concerned;

    b. The agreed resolution is such that the object of the complaint no longer exists; and

    c. The HmbBfDI will close off its file in this matter having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021.

Signed for and on behalf of the HmbBfDI:

02. February 2022

[redacted]

Hamburg DPA

LDA Brandenburg - S ahnsdor er Damm 77 - 14532 Kleinmachnow

Technology and Organisation

[redacted]

Date:	10 August 2021
Processor:	[redacted]
Phone:	[redacted]
Fax:	[redacted]
Sign:	[redacted]

(Please indica e charac ers when replying)

For information:
[redacted]

[redacted],
[redacted]

[redacted]

User registration on [redacted] website- Hearing according to § 28 para. 1 Administrative Procedure Act (VwVfG)[1]

- Our letter of 28 September 2020

Dear [redacted],

Thank you for your statement of 9 November 2020.

After a thorough assessment of your statement, we consider the matter closed.

Due to a present cross-border processing of personal data, we have already notified the decision in advance to other European supervisory authorities in the course of the One-Stop-Shop procedure pursuant to Art. 60 (3) of the General Data Protection Regulation (GDPR) . [2]

In the course of the procedure, a European supervisory authority informed us of their concerns regarding the technical and organisational measures taken. They were of the opinion that a security measure such as an email verification procedure or an equivalent measure to ensure that the owner of the email is indeed the person registering on the controller's platform and that

[1] Administrative Procedure Act (Verwaltungsverfahrensgesetz) in the version promulgated on 23 January 2003 (BGBl. I p. 102), as last amended by Article 5(25) of the Act of 21 June 2019 (BGBl. I p. 846).

[2] General Data Protection Regulation of 27 April 2016 (OJ EU L 119, 4 May 2016, p. 1; L 127, 23 May 2018, p. 2; L 74, 4 March 2021, p. 35).

the data processed by the controller are indeed accurate is state of the art and does not entail a disproportionate effort and cost for a controller, given its size and global reputation, to ensure an adequate level of security in relation to the risks for data subjects within the meaning of Article 32 of the GDPR.

We share this view.

Due to the relatively low volume of complaints on the part of [redacted] and the LDA regarding the facts at hand, we, in agreement with the European colleagues who expressed their concerns to us, refrain from taking further official measures (such as a measure within the meaning of Article 58 (2) of the GDPR) at this point in time. Depending on any further complaints regarding user registration on the [redacted] website to the LDA, we reserve the right to take prompt measures within the meaning of Article 58(2) of the GDPR.

If you have any questions, please do not hesitate to contact us by telephone.

With kind regards

[redacted]

Brandenburg Commissioner
for Data Protection and Access to Information

Final Decision

national reference	136/20/1276, 136/20/2192
case register no.	306316
Art. 56 procedure	143055
draft decision	306327
Revised draft decision	437344

I. Data breach description

The controller reported two personal data breaches pursuant to Article 33 of the GDPR in July 2020 and December 2020. The cause of both personal data breaches and the resulting notifications was based on a software error.

The first software error occurred in connection with the social login and was discovered by two German users who reported the error to the responsible party. A potential attacker would first have had to log in to the user's account with a correct username/password combination via a social login. The browser stores a token that would have confirmed the successful login with the social login at [redacted]. Then a potential attacker would have been asked for the name of the other person during an account change. If the attacker knew the username of another user and entered it during the account switching process, he could have logged into the other account. The software bug did not affect two-factor authentication. The discoverers of the bug accessed accounts from two commercial accounts for testing purposes, so the affected parties of the personal data breach in question are the two commercial sellers. Beyond that, no other affected parties are known. However, [redacted] assumes that the bug had already existed since 2018. The bug was reported on November 17, 2020 and directly fixed. A report to the responsible supervisory authority was obsolete at that time, because it was assumed that the bug occurred on the same computer of both discoverers. Therefore, after evaluating the bug and its scope, the notification was made on December 9, 2020. Successful inspection by the discoverers of the bug was made on the public username, name and business address of the company owner, in-formation on company turnover, obfuscated and shortened phone number and email address.

The second software bug occurred because - in addition to the name - the specified residential address of commercial sellers, which had to be specified or updated as part of the customer verification check, overwrote the registered business address in the [redacted] database and thus became visible on the platform. This affected approximately 1200 - 1300 commercial [redacted] sellers from Germany. According to [redacted], the number of affected sellers corresponds to [redacted] of [redacted] users in the EU. However, there are no known affected sellers from other European countries - according to [redacted], only German sellers are affected. The facts of the second software error are nevertheless the subject of this decision due to the similarity to the first software error.

II. Measures by [redacted] / risk assesment by [redacted]

In general, [redacted] has a comprehensive process for software development and testing. In particular, a "Software Development Life Cycle" (SDLC) process runs through various tests such as user acceptance tests, unit tests or functional automation tests. A final approval of the testing is given by QoS engineers. In addition, a release goes through a [redacted], in which a global information security team is significantly involved and decides on the subsequent implemen-ta-tion and testing and evaluation of the test results. Furthermore, [redacted] is com-mitted to (further) automating tests.

The cause of both software bugs was an error within the design and test phase of the software development cycle. The wrong data source was accidentally used for the application. There were also no noticeable bugs during the quality as-surance process or during the "production smoke tests".

As an immediate measure, all current projects were stopped and an investigation into the cause of the error was initiated. [redacted] assured to improve the software development process and especially the internal control of access to data. In addition, the API responsible for access would be improved and an immediate compulsion to call the API would be enacted.

III. Legal assessment

a. Decision of the Brandenburg Commissioner for Data Protection and Access to Information from June 7, 2021

We closed our first legal assessment with the following conclusion:

„Due to the measures taken immediately, the general measures within the meaning of Art. 32 of the GDPR and the fact that the Brandenburg Commissioner for Data Protection and Access to Information has not received any complaints within the meaning of Art. 77 of the GDPR for either software error, we consider the matter closed.“

b. Objection / comments by SA Poland

The SA Poland raised an objection to our draft decision from June 7, 2021.

SA Poland sees a violation of Art. 24 (1), 25 (1), 25 (2), 32 (1) and 32 (2) GDPR.

In the opinion of the Polish SA, a reprimand – pursuant to Art. 58 (2) lit. b GDPR – should be is-sued to [redacted] in connection with the violation of the provisions of the GDPR.

The SA Poland asks for the data on which the controller found the data breach and the date on which the competent supervisory authority was notified of each of the breaches. In this context the SA Poland asks for an assessment in regard to whether or not the controller has complied with Article 33 (1) GDPR.

The SA Poland also ask to indicate if the controller complied with Art. 34 (1) GDPR.

c. Revised Decision of the Brandenburg Commissioner for Data Protection and Access to Information

The Brandenburg Commissioner for Data Protection and Access to Information also sees a violation of Art. 24 (1), 32 (1) and 32 (2) GDPR because even there was a human error, further effective measures should have been taken to prevent the resulting data breach. Because of this structural error, the Brandenburg Commissioner sees an infringement.

The reason why we have not issued a reprimand in accordance with Article 58(2)(b) of the GDPR in the first place is that the SA Brandenburg is prohibited by national law (see § 43 (4) BDSG (Federal Data Protection Act)) from using the information made available by the controller in the context of the Art. 33 (1) GDPR notification.

After review of this case in the light of the RRO by the Polish SA and the second legal assessment we concluded that a reprimand according to the GDPR in the light of our national law is possible. For this reason the Brandenburg Commissioner will issue a reprimand.

With regard to the notification period within the meaning of Article 33 (1) GDPR, we were unable to identify any violation, as the period was within the 72 hours.

Since only name and email address were affected within the data breach, we do not assume a high risk in terms of Art. 34 (1) GDPR.

Since no further objection within the meaning of Article 60(4) GDPR was raised, we issue the administrative act of reprimand within the meaning of Article 60(5),6,7 GDPR and inform the data controller.

On behalf of the Brandenburg Commissioner for Data Protection and Access to Information,
September 29, 2022
Kleinmachnow, Germany

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

535.2009 / 631.442

13 March 2022

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller**: Fabletics GmbH (ehemals Just Fabulous GmbH), Fabletics.de, Schlesische Straße 38, 10997 Berlin
- **Incident:** Data of Fabletics users (fabletics.de, fabletics.co.uk, fabletics.es, fabletics.fr, fabletics.nl) were temporarily visible to other users due to a technical misconfiguration of the server
- **Date of occurrence**: 26 August 2020, 18:13 - 21:01 o'clock
- **Date of acknowledgement of the incident:** 26 August 2020, 20:04 o'clock
- **EU/EEA Member States concerned, with the number of data subjects concerned:**
  Germany: 283
  Spain: 35
  France: 144
  Netherlands: 28
  UK: 577
- **Category of data subjects:** customers of the online shops
- **Category of the data types/data records concerned:** Name, address, email address, phone number and account history
- **Likely consequences of the violation of the protection of personal data:** possible misuse of address data (e.g. data trading or for abusive transactions)

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

Data of Fabletics users (fabletics.de, fabletics.co.uk, fabletics.es, fabletics.fr, fabletics.nl) was temporarily visible to other users due to a technical misconfiguration of the server (incorrect configuration of a code in the load balancer to address Google Chrome "samesite" cookie policy).

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 faulty code has been removed in the load balancer, so the problem should not occur again (the controller also writes in the data breach notification that they do not want to use the faulty code again in a context that could affect the personal data of the customers.

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.

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/beschwerde.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

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

Yes, the affected customers were informed of the data breach by e-mail on 1 September 2020.

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

Deactivation of the faulty code and logout of all customers from the web shop so that they had to log in again and, if possible, no more customer data could be viewed through "open" logins.

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)

Permanent deactivation of the faulty software code

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, the Berlin DPA closes the case.

7.2. Examination of the intended measures with regard to the possible underlying data protection violation by the specialist unit.

In the light of the above-mentioned considerations, the Berlin DPA closes the case.

Berlin Commissioner
for Data Protection
and Freedom of Information

521.11505 / 631.189

CR: 117817

IMI RD 164070

Berlin, 02 June 2022

Final Decision

Preliminary remarks

The complaint (ref. no. 521.11505 / 631.189) was raised before the Berlin DPA in June 2019. It was transferred to the supervisory authority Netherlands, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by Nike European operations Netherlands B. V., in accordance with Article 56 GDPR. The LSA Netherlands conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. Following an objection to the Draft Decision, the LSA Netherlands proposed a Revised Draft Decision and thereby the complaint was rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

> With regard to the abovementioned cases and pursuant to Article 60(3) of the General Data Protection Regulation (GDPR), the Autoriteit Persoonsgegevens (Dutch Data Protection Authority, hereafter: NL SA) has issued the following revised draft decision:
>
> **Summary**

The NL SA has received the following complaint about the "Nike Run Club" app. According to the complainant the app does not allow to transfer his user data to another service (right of data portability).

On 26 June 2019, a complaint was filed with the Berliner Beauftragte für Datenschutz und Informationsfreiheit (hereafter Berlin SA) against Nike European Operations Netherlands B.V. The complainant would like to exercise his right to data portability by transferring his user data from the “Nike Run Club” app to another service. Allegedly the app this is not possible and the lack of this option was confirmed by the controller via phone on 26.06.2019. As the main establishment of Nike European Operations Netherlands B.V. is in the Netherlands, the NL SA is competent to act as the lead authority.
The Berlin SA forwarded this complaint to the NL SA.

Preliminary vetting by the Berlin SA
On 30 July 2019 the Berlin SA sent a request for information to Nike to inquire which DPA is competent for the processing of data portability requests. The request was answered by letter dated on 30 September 2019. In the reply Nike wrote that the right to data portability can be exercised and that in the previous four month, Nike had received 127 data portability requests and that no issues or complaints were known in connection with the requests for data portability.

Norm allegedly infringed

- Article 12 (2) GDPR states that the controller shall facilitate the exercise of data subject rights under Articles 15 to 22 GDPR.
- Article 20 (1) GDPR states that the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller [...].

The complainant states that he could not exercise this right.

Investigation by the NL SA
The information collected by the vetting action of the Berlin SA was assessed by the NL SA. The NL SA then investigated the websites related to the Nike Run Club. According to page 5

of the privacy policy of the app, under the header "PROTECTION and MANAGEMENT of your Personal Data" >> "Managing your personal data", the user does have the option to receive an electronic copy of his personal data (data portability). The website has a web form to exercise this right.
http://agreementservice.svs.nike.com/rest/agreement?agreementType=privacyPolicy&uxId=com.nike.commerce.nikedotcom.web&country=UK (replace UK with DE for the same page in German).

On 30 September 2020 the NL SA sent an information request to Nike to inquire (1) since when Nike's German website has been offering the right to data portability, and (2) whether this service suffered any interruptions during the month of June 2019. On 15 October 2020 Nike replied that (1) the German website offers the right to data portability using the web form since 4 June 2018, and (2) that in June 2019 no planned or unplanned service interruptions occurred that might hinder German data subjects in exercising their right to data portability. Nike shared screenshots that show the exact number of request regarding the right to data portability in the European Union in the period 29 April 2019 to 5 August 2019. The screenshots show a consistent pattern of requests, without descending or overflow that could indicate disturbances.

Additionally the Dutch DPA has not received any complaints about Nike regarding the right to data portability. Also desk research did not reveal any issues with functioning of the data portability of this app.[1]

Proposed action by the NL SA

Based on the privacy police that the NL SA found on the app, in addition to the information provided by Nike to the Berlin SA, and the information provided by Nike to the NL SA, the NL SA conclude that Nike does facilitate that a data subject is able to receive his personal data in a structured, commonly used and machine-readable format pursuant to Art. 20 (1) GDPR. Therefore the NL SA did not identify any infringement of the obligations set out in the GDPR. The complaint has only a limited personal impact, and the NL SA has no indication of structural short comings of the company. In view of the above, appropriate action has been undertaken and no further action is required.

[1] E.g. the Google search with key words nike run club data portability reveals many articles and tutorials on the functionality.

Henceforth, the cross-border complaint case (national reference 521.11505 / 631.189) should be closed.

Appeal Notice to the complainant

Against this decision a lawsuit before the Verwaltungsgericht Berlin (administrative court of Berlin), Kirchstraße 7, 10557 Berlin is admissible. The lawsuit needs to be filed in written form within one month after the notification of this decision, it can also be filed as an electronic document with a qualified electronic signature (QES) or for the record of the clerk of the court. Please, note that in case of filing the lawsuit in writing the legal deadline is only met if the lawsuit reaches the administrative court within the deadline.

The Berlin Commissioner for Data Protection
and Freedom of Information

Berlin Commissioner
for Data Protection
and Freedom of Information

521. 12549/ 631.196

CR: 74063

Draft Decision
IMI DD 418292

Berlin, 24 August 2022

Final Decision

Preliminary remarks

The complaint (ref. no. 521. 12549/ 631.196) was raised before the Berlin DPA inFebruary 2020. It was transferred to the supervisory authority Netherlands, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by [redacted], in accordance with Article 56 GDPR. The LSA Netherlands conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. The LSA Netherlands proposed a Draft Decision and thereby the complaint was rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

IMI Article 56 identification of LSA and CSA entry	114902
IMI Case Register entry	418274
National file number	NL SA: z2021-05733
Controller	[redacted]
Date of complaint	19 February 2020

With regard to the abovementioned case and pursuant to Article 60(3) of the General Data Protection Regulation (GDPR), the Autoriteit Persoonsgegevens (Dutch Data Protection Authority, hereafter: NL SA) has issued the following draft decision:

Summary of the complaint

1. NL SA has received a complaint about telephone recordings without the consent of the complainant from the Berlin regulator under our file number z2021-05733. The person concerned ([redacted] pleads the alleged infringement of the GDPR. It follows from the complaint file that [redacted] is concerned that the controller [redacted] may have recorded a telephone call between him and a customer service employee. The complainant objects to this processing of data concerning him.

2. The Dutch Data Protection Authority (AP) has received this complaint on 30 April 2020.

Investigation by NL SA

3. NL SA has established that [redacted] The Netherlands, is the data controller in this matter. This is confirmed by, inter alia, the correspondence received from [redacted] and the privacy policy on [redacted]

4. On the 10 May 2021, the NL SA sent an information request to the controller regarding this case. In the request for information, the NL SA submitted the complaint.

5. On 31 May 2021, the controller replied: *We have reviewed our systems, but we have not found any information indicating that we have ever received a complaint from* [redacted] *at our special privacy email address* [redacted] *It therefore seems that* [redacted] *did not seek to raise his concerns directly to us, nor gave us the opportunity to respond to those concerns, but instead immediately expressed his concern to*

the Berlin regulator.

6. [redacted] also stated: "*We have been able to find a phone call that took place on February* [redacted] *linked to the account created for* [redacted] *Our details confirm that this phone call has not been recorded. We are sorry to hear that our customer service officer has created ambiguity at* [redacted] *Since there is no call recording available, we cannot confirm that the content of the conversation took place as* [redacted] *described it. In any case, we will review our guidelines for our customer service staff on call recordings. We can also confirm that the statement "for security purposes shall be recorded, without exception" is incorrect.*

7. The NL SA has received no prior information from Berlin SA derived from the preliminary vetting of the complaint.

Norm allegedly infringed

Art. 6 GDPR jo article 12, 13, 21 GDPR

Proposed action by the NL SA

1. Firstly the NL SA would like to point out that the lodged complaint was premature as the request for erasure was apparently sent directly to the regulatory authority in Berlin, and not to the company itself.

2. Secondly, there is no clear indication that there is an enforceable obligation on the controller to handle the request of [redacted] under the current circumstances. The controller needs to respond to data subject requests without undue delay - and in any case within one month from the receipt of a request. However, no such request is available. Only in the case of the controller's inactivity or refusal to fulfill the request in part or in whole, there is a title to lodge a complaint with referring to an infringement of article 21 jo. article 12, para 3, of the GDPR.

3. Thirdly, NL SA is unable to establish whether call recordings have taken place involving the complainant.

4. Furthermore, the NL SA has no indication that the controller is unwilling to facilitate data subject requests. In this case [redacted] informed the NL SA within one month about their view on the matter.(the letter dated 31 May 2021 after the NL SA's information request on 10 May 2021).

5. Considering above, NL SA considers that there is no evident infringement of the GDPR in this case. ▪

6. NL SA deems this matter investigated to the extend appropriate and rejects the complaint based ex article 60, para 8, GDPR. The supervisory authority with which the complaint was lodged (the regulatory authority in Berlin) shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

The Hague,
12th of July 2022

Appeal Notice to the complainant

Against this decision a lawsuit before the Verwaltungsgericht Berlin (administrative court of Berlin), Kirchstraße 7, 10557 Berlin is admissible. The lawsuit needs to be filed in written form within one month after the notification of this decision, it can also be filed as an electronic document with a qualified electronic signature (QES) or for the record of the clerk of the court. Please, note that in case of filing the lawsuit in writing the legal deadline is only met if the lawsuit reaches the administrative court within the deadline.

The Berlin Commissioner for Data Protection and Freedom of Information

Berlin Commissioner
for Data Protection
and Freedom of Information

631.457.4
521.14765.10

CR 378706

IC 392914

DD 405582

09 August 2022

Final Decision

Reprimand

Your undated letter, received by us on 6 April 2022.

Dear Sir or Madam,

We hereby issue a reprimand to your company for infringements of the General Data Protection Regulation (GDPR).

Reasoning:

Our decision is based on the following considerations:

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Friedrichstr. 219, 10969 Berlin
Visitors' entrance: Puttkamerstr. 16-18

Phone: (030) 13889-0
Fax: (030) 215 50 50

Office hours: Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm

Mail: mailbox@datenschutz-berlin.de
Web: www.datenschutz-berlin.de

BERLIN

I.

We have established the following facts:

The complainant in the proceedings with the above-mentioned reference informed us that she had received an order confirmation from a company called "Healy" to her e-mail address [redacted]. She assumed that a customer of your company had given an incorrect e-mail address (the complainant's e-mail address) when placing the order. The complainant had informed your company by e-mail that the e-mail address used was incorrect. Your company did not react to this information. The complainant had also received shipping confirmations with personal data of the actual customer as well as Healy newsletters to her e-mail address. The complainant provided us with examples of emails written in English that she had received in July 2021 from service@healy.de, no-reply@healyworld.net, your.healy@healy.shop and no-reply-healy-world@healy-world.net. In addition, she had received information in German from healy@globalewallet.com about a credit balance including the password and user name of another person.

The complainant requested your company by e-mail (dated 28 June and 6 July 2021) to delete her e-mail address. She then received an e-mail from your company telling her to log into her - in fact non-existent - customer account and fill in a form there.

In a letter dated 22 February 2022, we asked you to comment on the facts described and also consulted you on our intention to issue a reprimand to your company.

In a letter received by us on 6 April 2022, your company confirmed that the complainant had received emails from your company. This was due to a faulty process in your company's back office. There had been a customer in your company's database with the same name as the complainant. In her customer account, the manual entry of the e-mail address by the responsible employee, the e-mail address of the complainant [redacted] instead of the e-mail address of the customer [redacted]. After your company had become aware of the complainant's complaint, the process of creating the customer account had been completely automated, so that manual data entry by your company's employees was no longer possible. Moreover, a double opt-in procedure had been implemented for the customer e-mail registration in order to prevent incorrect e-mail addresses from being assigned to a customer account.

At first, your company did not comply with the complainant's request for erasure because the customer service department was of the opinion that the e-mail address to be erased was your

customer's e-mail address and that the e-mail address was still required to process an open order and open commission claims. Moreover, the complainant had not addressed her request for deletion to your company's data protection officer, but to Healy's customer service, which had only forwarded her request to the legal department after a delay. The complainant's e-mail address had been deleted on 4 August 2021, after you had become aware of the complaint. The complainant was sent an email apologising on 23 September 2021. In September 2021, the customer service had again been trained in the handling of personal data and an e-mail address had been created so that the external data protection officer of your company could be contacted.

II.

Legally, we assess the facts as follows: Your company has infringed the GDPR.

1. Personal data may only be processed if the person responsible for the processing can refer to a legal basis. In the present case, there was no legal basis for the processing of the complainant's e-mail address, so that your company infringed Art. 6 GDPR.

2. According to the first sentence of Art. 12(3) GDPR, the controller must provide the data subject with information on the measures taken upon requests pursuant to Articles 15 to 22 GDPR without undue delay, and in any event within one month of receipt of the request. Your company did not respond to the complainant's request for erasure of 28 June and 6 July 2021 within the one-month period, so that there is also an infringement of the first sentence of Art. 12(3) and Art. 17 GDPR. The fact that the complainant did not address her request for erasure to your company's data protection officer but to Healy's customer service does not justify the failure to reply in time. There is no obligation in the GDPR for data subjects to assert their data protection rights electronically, nor is there an obligation to send requests only to a specific e-mail address. Rather, the second sentence of Art. 15(3) GDPR states:

   > "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."

The complainant could therefore also have submitted her request for erasure by other means, e.g. by post. The right to erasure is directed against the controller pursuant to Article 17(1) of the GDPR. The complainant sent her request for erasure to an e-mail address used by your company.

III.

As a result, we decided not to take any further supervisory measures due to the infringement, but to leave it at a reprimand for the time being.

The reprimand is based on Art. 58 (2) (b) GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after completing our investigation. We identified an infringement on your part for the first time. When approached by us, you showed understanding and informed us that you had already taken measures to prevent a recurrence of the incidents complained about.

In the certain expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

Legal Remedies

An action against this decision may be brought before the Berlin Administrative Court. It must be lodged in writing - also as an electronic document by means of a qualified electronic signature (QES) - or with the clerk of the court within one month of notification of this decision at the Berlin Administrative Court, Kirchstraße 7, 10557 Berlin. Please note that in the case of a written complaint, the time limit for filing a complaint is only met if the complaint is received by the administrative court within this time limit.

Yours sincerely

Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

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.

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/beschwerde.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

521.10344.26
631.65
CR 85084
DD 339845
IC 416091
RD 431505

14 September 2022

FINAL DECISION

[redacted]

To the legal representation of [redacted]

Reprimand
Your letters of 21 October 2021, of 21 December 2021 and of 8 June 2022

Dear [redacted],

We hereby issue a reprimand to [redacted] for an infringement of the General Data Protection Regulation (GDPR).

Reasoning:

Our decision is based on the following considerations:

I.
We have established the following facts:

The complainant states that [redacted] asked him to update his postal address when he registered for his existing customer account on the company's website on 2 October 2018. In doing so, a telephone number was also collected as a mandatory field. The complainant objects to the compulsory collection of his telephone number as a mandatory field. He sees this as an infringement of the provisions of the GDPR.

The practice of processing telephone numbers has – based on the complaint discussed here – been the subject of correspondence with you and your client for some time (our reference 501.118). According to your client's statement (your letter of 18 March 2020), a telephone number is compulsorily collected from the d when a new means of payment is created. We therefore assume that the complainant's statement of the facts is correct.

be Berlin

The complainant's statement of the facts was not disputed by you or your client in your letter of 21 October 2021 mentioned above.

In its letter of 19 November 2018, [redacted] informed us that it uses the telephone numbers in its customer service if a user has a problem that cannot be solved by e-mail or chat. In such cases, the employees [redacted] also support the users personally on the phone. The letter further states that the collection of the telephone number was permissible under Article 6 (1) GDPR.

In its letter of 12 March 2019, [redacted] adds that the relevant legal basis is "contractual performance". We therefore assume that [redacted] bases the collection of the telephone number as a mandatory field for ordering processes in its internet offer on Art. 6 (1) (b) GDPR.

In your letter of 18 March 2020, you also state that the collection of the telephone number as a mandatory field is necessary when a means of payment is created for preventing misuse or fraud. Thus, in the event of suspected third-party access to a customer's account or in the event of an incorrect debit and corresponding blocking of the account, "... so that access via e-mail address is no longer possible ..." the customer could be notified by SMS. Against this background, the processing of the telephone number and its collection as a mandatory field when registering a means of payment was, according to you, necessary for the implementation of your client's user contracts and thus permissible under Article 6(1)(b) GDPR.

In your letter of 6 January 2021, you further add that the protection of customers is one of the contractual accessory obligations that [redacted] must fulfil towards its customers. Sufficient and equally effective protection could not be achieved solely by using the deposited e-mail address as a means of contact.

You state that it is recognised in the legal literature that the characteristic "necessity" should not be interpreted too narrowly and that the examination therefore does not require consideration of the principle of proportionality. Data processing would also be necessary if it appears reasonable from the objective point of view of a reasonable third party.

Furthermore, according to you, the processing of the telephone number was also proportionate in a narrower sense and thus necessary: only the telephone number would enable a quick and direct contact with the customers in the event of possible misuse. If [redacted] could only inform the customer by e-mail, such contact would take several hours or - if a customer was absent, for example, due to holidays or other reasons - even several days.

In addition, you state, that contacting the customer by e-mail in the event of misuse would not be effective in those cases where there may have been unauthorised access to the customer's e-mail account as well. It is not beyond life experience that a customer may use the same password for several accounts. In such cases, unauthorised access is also possible to the customer's e-mail account. This does not make it impossible to notify the customer by e-mail, but it does not make it as secure as contacting the customer by telephone. In your experience, hacking a mobile phone still requires more effort than hacking an e-mail account or any other user account.

In addition, only a telephone call would allow a quick authentication of the customer, as the customer could authenticate himself to [redacted] customer service, for example, by giving his date of birth or other details. This, too, could not be guaranteed by contacting the customer by e-mail. You further state that the data protection authorities recognised that the telephone number is used, for example, when asserting data subjects' rights, in order to clearly identify the data subject. For example, in the banking or telecommunications sector, but also in other areas, contact by telephone is not unusual in order to ensure additional security.

Alternatively, you claim, the practice of your client described above could be based on its legitimate interests within the scope of Article 6(1)(f) GDPR.

With regard to our letter of 30 September 2021 (reference: 521.10344.10) prior to this reprimand, you informed us in your above-mentioned letter of 21 October 2021 that your client had already initiated the process of erasing the complainant's telephone number. You confirmed the erasure of the complainant's telephone number on 21 December 2021 and its notification on the same day to us in a letter dated 8 June 2022.

II.
Legally, we assess the facts as follows: [redacted] has infringed the GDPR.

1. <u>Processing of the telephone number for the performance of the contract (Art. 6 (1) (b) GDPR)</u>

a. Processing of the telephone number for customer service purposes

Art. 6 (1) (b) GDPR cannot be considered as a legal basis for the performance of customer service in the present case, as the mandatory provision of the telephone number is not necessary for the performance of customer service within the scope of the aforementioned regulation. The other communication channels available to [redacted] (and in particular the possibility for data subjects to contact [redacted] themselves by telephone or email for customer service purposes) are sufficient for these purposes.

In its current guidelines on Article 6(1)(b) GDPR, the European Data Protection Board also assumes for online services that this general permission cannot justify data processing for purposes of service improvement (Guidelines 2/2019 for the processing of personal data pursuant to Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, 8 October 2019, para 49).

b. Processing of telephone numbers to combat fraud and abuse

Also the processing of personal data for the purpose of combating fraud and abuse cannot be based on Art. 6 (1) (b) GDPR:

aa) The legislator itself already classifies the processing of personal data to the extent strictly necessary for the prevention of fraud as a legitimate interest of the respective controller (recital 47, sentence 6).

bb) The Art. 29 working party had already stated with regard to the largely identical provision in Art. 7 of Directive 95/46/EC that the fight against fraud was a "... further typical area which is likely to go beyond

what can be regarded as necessary for the performance of the contract" (Art. 29 Working Party, WP 217, p. 22) and declared only consent, a legal obligation or a legitimate interest of the controller (Article 7(a), (c) or (f) of Directive 95/46/EC) applicable as a legal basis. This interpretation of the Article 29 Working Party has been reaffirmed by the European Data Protection Board (EDPB) for the provision of online services to data subjects (Guidelines 2/2019, version 2.0, October 2018, para. 28 f.).

cc) It is also recognised in the legal literature that fraud or abuse prevention cannot be based on Art. 6 (1) sentence 1 lit. b GDPR.

dd) According to the explanations in its privacy policy, your client itself also considers the detection and prevention of fraud and abuse - correctly - as its legitimate business interest [redacted]

In summary, Art. 6 (1) (b) GDPR cannot be considered as a legal basis for the implementation of the customer service or for the prevention of abuse or fraud.

2. <u>Processing of the telephone number based on Art. 6 (1) (f) GDPR</u>

The obligatory provision of the telephone number for the performance of customer service and/or for the prevention of abuse or fraud cannot be based on Art. 6 (1) (f) GDPR:

a. Processing of the telephone number for customer service purposes

It is true that [redacted] has a legitimate - economic - interest in collecting and processing the telephone number in the context of customer service in order to ensure customer satisfaction. However, the necessity for the compulsory collection of the telephone number is lacking.

Regarding the term necessity, the Conference of Independent Data Protection Authorities of the Federation and the Länder states in its guidance for telemedia providers (as of March 2019, p. 13): "Necessity means that the processing is **suitable** to achieve the interest (motive/benefit of the processing) of the controller, **whereby no milder, equally effective means is available**. This means that the controller must limit the processing to what is necessary" (emphasis by the author).

In addition, the overriding objective of Art. 5 (1) (c) GDPR ("data minimisation") must be taken into account when interpreting the provision.

There is therefore no room for an expansion of the concept of necessity - as proposed in your letter of 6 January 2021 ("... necessary and thus also required is the data processing even if it appears reasonable from the objective point of view of a reasonable third party") - even if this is occasionally advocated in the legal literature. This legal opinion is

based on interpreting a European law concept according to the standards of German law. According to the established case law of the CJEU, this is inadmissible.

The processing of the telephone number is also not, as you state in your letter of 6 January 2021, "proportionate in the strict sense and thus necessary":

Customer satisfaction can just as well be ensured by [redacted] making it optional for its customers to provide a telephone number for the aforementioned purposes, so that those customers who wish to make use of this service offer can provide their telephone number and those customers who do not wish to do so do not have to do so. This is a milder and equally effective means compared to the compulsory processing of the telephone number for customer service purposes.

As a result, the compulsory collection and further processing of the telephone number of the data subject for customer service purposes is not necessary and can therefore not be based on Art. 6 (1) (f) GDPR.

b. Processing of telephone numbers to combat fraud and abuse

It is true [redacted] has a legitimate - economic - interest in collecting and processing the telephone number to combat fraud and abuse. However, the mandatory collection of the telephone number lacks the necessity required by law for lawfulness also here.

The processing of the telephone number for this purpose is also not, as stated by you in your letter of 6 January 2021, "proportionate in the strict sense and thus necessary":

The description of this in your letter of 6 January 2021 apparently assumes that the company's customers can be reached by telephone at any time. This in itself contradicts general life experience, especially in the case of working people. Thus, with regard to the entirety of the customers, there are already doubts about the suitability of the processing with regard to the intention declared by your client to contact the customers "in real time" in case of suspicion of fraud or abuse.

At the same time, you state that a notification by e-mail could take hours or even days in the case of absence due to holidays. We consider this assumption incorrect as well. On the contrary, large parts of your client’s customers probably have a smartphone and use your client's services via it. These devices also allow the immediate receipt of e-mails - even while on holiday. The additional processing of the telephone number for sending SMS is therefore undoubtedly not necessary, at least with regard to these customers. Furthermore, your client is free to send the notifications in question to the customers via the apps of your client's company used by these customers.

This means that the vast majority of customers should be able to be notified in the event of fraud and abuse without the compulsory collection and use of a telephone number.

In addition, when using landline telephone numbers, it should be noted that your argumentation does not apply in this respect.

Your client is also free to obtain the (voluntary) consent of those customers who cannot be reached in this way, after informing them of the intended processing.

Also, when using the e-mail addresses stored by the customers for their notification in case of suspected fraud or misuse, there is usually no additional requirement for their authentication, as you seem to assume (your letter of 6 January 2021, page 4, 2nd paragraph).

As a result, the above-mentioned measures provide your client with milder and equally effective means to realise its legitimate interest in combating fraud and abuse. Forced processing of the telephone number is therefore not necessary within the scope of Article 6 (1) (f) GDPR.

Even if, in the case of Art. 6 (1) (f) GDPR, one were to assume a necessity and thus a legitimate interest of your client, the weighing of legal interests would in any case be to the detriment of your client. The interest or fundamental rights and freedoms of the data subject in not providing his or her telephone number outweigh the legitimate interests of your client in collecting compulsorily the telephone number for the purpose of customer service and for the prevention of abuse or fraud. Here, too, it must be taken into account - to the detriment of your client - that it can resort to other communication channels for the aforementioned purposes. In addition, the protection of your client's financial interests is satisfied by blocking the affected accounts. In this case, the blocking is at the expense of the data subject whose account has been misused. As soon as he or she has an interest in the further use of your client's services, he or she can be informed directly by your client anyway, including the possibility of offering telephone contact if necessary.

With the measures outlined above, a certain number of customers may remain in relation to the total number of customers of the company who do not give their consent to the processing of a telephone number for the purpose of fraud and abuse prevention. However, the decision on this must be left to the individual customers. The fact that it may not be possible to contact all clients immediately in the event of an attempt at fraud or abuse suspected by your client does not justify the compulsory processing of the telephone numbers of all clients.

As a result, the compulsory processing of a telephone number of customers of [redacted] for the purposes of customer service or the prevention of fraud and abuse can neither be based on Art. 6 (1) (b) GDPR nor on Art. 6 (1) (f) GDPR.

3. <u>Processing of the telephone number based on Art. 6 (1) (a) GDPR</u>

In this respect, the only possible legal basis for the processing of the telephone number in the context of orders on your client's website is consent pursuant to Art. 6 (1) (a) GDPR. Consent within the scope of the GDPR must be a **voluntary** expression of will "... for the specific case, given in an informed manner and in an unambiguous manner ..." (Art. 4 (11) GDPR), which must also fulfil the conditions of Art. 7 GDPR. Consent would also have to be designed in such a way that it can be given separately for the named processing purposes (customer service on the one hand and fraud and abuse prevention on the other).

However, according to the information available to us, [redacted] did not obtain the complainant's legally valid consent to the collection and processing of his telephone number at all in the present case.

4. Result

The processing of the complainant's telephone number for customer service purposes and to combat fraud and abuse cannot be based on either Art. 6(1) (b) or Art. 6 (1) (f) GDPR. Moreover, your client has not obtained legally valid consent from the complainant for this. No other legal basis is apparent.

The processing of the complainant's telephone number for customer service purposes and to combat fraud and abuse thus took place without the necessary legal basis and infringed the provisions of the GDPR (Art. 5 (1) (a), 6 (1) GDPR).

At the same time, the compulsory processing of the complainant's telephone number breached your client's obligation to minimise data under Art. 5 (1) (c) GDPR.

Your client was therefore obliged to delete the complainant's telephone number, as it was or is being processed unlawfully (Art. 17 (1) (d) GDPR).

III.
As a result, we decided not to take any further supervisory measures due to the infringement in this individual case, but to leave it at a reprimand for the time being.

The reprimand is based on Article 58 (2) (b) GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after completing our investigation. This is the first time we have identified such a breach by [redacted]. When approached by us, your client was reasonable, deleted the complainant's telephone number and informed the complainant accordingly without delay after the erasure had taken place.

With regard to the present individual complaint,, we thus consider the matter to be closed.

However, based on the correspondence with you and your client on the matter to date, we also assume that the compulsory collection and use of telephone numbers is not only taking place in the individual case in question here, but is rather a common practice on the part of your client. We recommend that your client immediately check this and also immediately delete the other telephone numbers of other clients that may have been stored without a legal basis (i.e. without the effective consent of the data subjects). We will review your client's general practice with regard to the collection and use of telephone numbers in the near future, also irrespectively of complaints. Should we find continued infringements of the applicable data protection law, we expressly reserve the right to take further supervisory measures.

Legal Remedies

An action against this decision may be brought before the Berlin Administrative Court. It must be filed in writing - also as an electronic document by means of a qualified electronic signature (QES) - or with the clerk of the court within one month of notification of this decision at the Berlin Administrative Court, Kirchstraße 7, 10557 Berlin. It is pointed out that in the case of filing an action in writing, the time limit for filing an action is only met if the action is received by the Administrative Court within this time limit.

Kind regards,