Litigation Chamber

Decision on the merits 183/2022 of 14 December 2022

File number: DOS-2022-00365

Subject: Communication of personal data to third parties without the

consent of the data subject

The Litigation Chamber of

the Data Protection Authority, composed of

Mr Hielke Hijmans, Chairman, and Messrs Frank De Smet and Dirk Van Der Kelen,

members ;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the

protection of natural persons with regard to the processing of personal data and

to the free movement of such data, and repealing Directive 95/46/EC (General Regulation on the

data protection), hereinafter "GDPR";

Considering the law of December 3, 2017 establishing the Data Protection Authority, hereinafter

"LCA";

Having regard to the internal regulations as approved by the House of Representatives on

December 20, 2018 and published in the Belgian Official Gazette on January 15, 2019;

Considering the documents in the file;

Made the following decision regarding:

The complainant:

Madame X, hereinafter “the complainant”;

The defendant: Y, represented by Me Heidi Waem and Me Simon Verschaeve, whose offices

are located at 1000 Brussels, rue aux Laines 70, hereinafter “the defendant”.

I. Facts and procedure

1.

On January 19, 2022, the complainant lodged a complaint with the Authority for the Protection of

given against the defendant.

Decision on the merits 183/2022 - 2/19

The plaintiff sought the services of the defendant - with whom she had

take out legal protection insurance - for the legal settlement of a car accident

traffic of which she had been the victim. As part of the settlement of this claim, the plaintiff

appointed a lawyer. Correspondence was exchanged between the defendant and the lawyer

of the plaintiff in the context of a dispute concerning the request for intervention of the

defendant by the plaintiff in the fees and other expenses occasioned by this

juridic assistance.

Due to human error, an employee sent an email regarding this support

to an incorrect email address on June 2, 2021. This email contained the following data:

the surname and first name of the complainant, the complainant's lawyer, the file number, the

installments paid, the fact that the person concerned has had an accident resulting in

injuries, the progress of the file and the dispute as to whether or not Y intervened as

as a legal protection insurer. The email did not include attachments.

On Friday, June 4, 2021, the defendant's DPO was contacted by the employee

involved in the incident and an internal investigation was immediately opened. Monday

June 7, 2021 at 2:58 p.m., the information necessary to adequately determine the

nature of the incident were obtained, after which the internal investigation was closed by the

competent service (Data Protection Unit) at 3:38 p.m. The notification to the DPA took place on the same

day at 9:17 p.m.

The defendant also contacted the wrong addressee on Monday June 7, 2021,

asking to destroy the e-mail and not to share the information with third parties,

transmit, store or use them in any way.

The complainant was then informed, on Tuesday, June 8, 2021, that a data breach had

produced. Finally, the defendant also contacted the plaintiff's lawyer on

June 9, 2021.

2.

On February 14, 2022, the complaint was declared admissible by the Front Line Service on the

basis of Articles 58 and 60 of the LCA and the complaint is forwarded to the Litigation Chamber

under article 62, § 1 of the LCA.

3.

On March 11, 2022, in accordance with Article 96, § 1 of the LCA, the Chamber's request

Litigation to proceed with an investigation is forwarded to the Inspection Service, as well

as the complaint and the inventory of parts.

4.

On April 14, 2022, the investigation by the Inspection Service is closed, the report is attached to the file

and this is forwarded by the Inspector General to the President of the Litigation Chamber

(article 91, § 1 and § 2 of the LCA).

The report contains findings relating to the subject of the complaint and concludes that:

1. a violation of Article 5, paragraph 1, a) c) and f) and paragraph 2, of Article 6,

paragraph 1, Article 24, paragraph 1 and Article 25, paragraphs 1 and 2 of the

GDPR in the context of the complaint in this case;

2.

the absence of a general infringement of Article 5, Article 24, paragraph 1 and

Article 25, paragraphs 1 and 2 of the GDPR;

3. a violation of Articles 33 and 34 of the GDPR.

The report also contains findings that go beyond the scope of the complaint.

The Inspection Service notes, in general terms, that:

4.

there is no violation of Article 38(1) or Article 39 GDPR;

5.

On April 29, 2022, the Litigation Chamber decides, pursuant to Article 95, § 1, 1° and article 98 of the LCA, that the case can be dealt with on the merits.

6.

On April 29, 2022, the parties concerned are informed by registered mail of the provisions as set out in article 95, § 2 as well as in article 98 of the LCA. The parts concerned are also informed, pursuant to Article 99 of the LCA, of the deadlines for report their findings.

For findings relating to the subject of the complaint, the deadline for receipt of conclusions in response of the defendant was set for June 10, 2022, that for the conclusions in reply of the complainant on July 1, 2022 and finally that for the conclusions in reply of the defendant on July 22, 2022.

7.

On April 29, 2022, the complainant accepts all communications relating to the case by way of electronic.

8.

On April 29, 2022, the defendant accepts all communications relating to the case by electronic way.

9.

On May 20, 2022, the defendant requests a copy of the file (art. 95, § 2, 3° of the LCA), which was transmitted to him on May 23, 2022.

10. On June 10, 2022, the Litigation Chamber receives the submissions in response from the defendant regarding the findings relating to the subject-matter of the complaint. These findings also include the defendant's reaction to the findings carried out by the Inspection Service outside the framework of the complaint. Mainly, the

defendant argues that the procedure and its terms of execution by the Service

d'Inspection and the Litigation Chamber violate the general principles of good

administration. In the alternative, the defendant maintains that this violation concerning

personal data does not constitute a violation of the principles of lawfulness,

GDPR Data Minimization, Integrity and Privacy. Furthermore, the

defendant did not violate the GDPR following the notification of the data leak to the DPA and to

the person concerned.

11. On July 14, 2022, the Litigation Chamber confirms to the defendant that the complainant has not

did not submit any rebuttal submissions with respect to the findings relating to

the subject of the complaint.

12. On July 20, 2022, the Litigation Chamber received notification from the defendant according to

which it will not introduce conclusions in reply.

II. Motivation

II.1. Principles of good administration

13. Respondent argues that both the procedure and the manner in which it was carried out by the

Inspection Service and

the Violent Litigation Chamber

the principles of good

administration. The defendant submits that by the manner in which the complaint was examined,

the Inspection Service and the Litigation Chamber violated the precautionary principle.

The Litigation Chamber did so in particular by deciding that an investigation by the Service

of Inspection was required in this case. The Inspection Service would have violated these

principles in deciding to extend the scope of the investigation beyond the subject of the

complaint. The defendant also asserts that the principles of reasonableness and

proportionality have been violated. This aforementioned extension of the scope

dealt with aspects that had already been questioned and examined recently in

in the context of another investigation by the Inspection Service and for which the Inspection Service

found no violations.

14. In this respect, the Litigation Division observes that it has indeed decided to seize the

Inspection service in order to carry out an investigation on the basis of article 94, 1° of the LCA.

The Litigation Chamber assesses in each file both the consequences

personal potential for a complainant and the social consequences of the treatment

litigious.

This case concerns a personal data breach

(data leak). Personal data breaches are a problem

per se, but can also be symptomatic of a security system of

vulnerable or even obsolete data. In addition, these violations may indicate weaknesses

in the system, which should be remedied if necessary.

15. The Litigation Chamber recalls that a complaint rarely gives a complete picture or

objective of a treatment or of a situation denounced by the complainant. Since the Chamber

Litigation did not have all the information on the relevant facts on the basis

of the complaint, it requested an investigation by the Inspection Service. In this context, the

Litigation Chamber emphasizes that an inspection is therefore not always requested in

intent to necessarily establish a violation, but rather to gain insight as

accurate as possible of the relevant objective facts. The investigation by the Inspection Service may

just as well to exclude a violation as to establish it. The investigation is therefore carried out against and

at discharge.

16. The Respondent submits that it is clear from the Complaint itself that the violation

of personal data is the result of human error, which is apparent

also retrospectively of the inspection report. Although it appears from the report

inspection that the personal data breach is indeed in this case the
consequence of a human error, the Litigation Chamber emphasizes that it was unable to
establish it with total certainty beforehand and that he cannot be blamed for having thus
requested an investigation in order to obtain a full and accurate overview of the circumstances in
which the personal data breach occurred. More generally, the
Litigation Chamber emphasizes that the decision on the follow-up of a file in accordance with
Article 95, § 1 of the LCA constitutes a necessary intermediate step in this
procedure that the Litigation Chamber must be able to take in complete freedom.
17. The defendant also argues that the Litigation Chamber should have dismissed the
complaint dismissed on the basis of its dismissal policy, in particular the reason
B.3 "Your complaint is ancillary to a larger dispute which requires
to be argued before the courts and judicial and administrative tribunals or another
competent authority". In this context, the Litigation Chamber recalls that it is not
obliged to classify these complaints without follow-up but that it enjoys the discretionary power
to examine individually for each complaint whether it will close it without follow-up or not. In the
present case, it was decided not to dismiss this complaint but the Chamber
Contentious decided to seize the Inspection Service for the following reasons. In his capacity
as a legal protection insurer, the defendant processes sensitive data of the
persons concerned. The defendant also processes this data on a large scale. He is
therefore important that sufficient guarantees, such as for example in terms of
confidentiality, are provided by the defendant so that these large-scale processing operations
scale of sensitive personal data are carried out in compliance with the
fundamentals of the GDPR.
18.
The Litigation Chamber wishes to further clarify this point, without prejudging the analysis
the facts underlying the complaint and the possible breaches of the GDPR that could

result. The Litigation Chamber refers for this purpose to article 100 of the LCA1, where its decision-making competence is defined within the framework of a procedure on the merits. This provision explicitly provides that, in addition to a series of other measures,

bedroom

Litigation has the possibility of filing a complaint without follow-up (article 100, § 1, 1° of the LCA), also in the proceedings on the merits. The Litigation Chamber emphasizes that it is permissible, even in this phase, to classify complaints without follow-up for reasons technical or expediency reasons, in accordance with the conditions set out in the jurisprudence of the Court of Markets.2

19. The defendant also argues that the Inspection Service breached the duty of diligence in deciding to further expand the scope of the investigation. This extension of the field of application also covered aspects which had already been questioned and recently examined as part of another investigation by the Inspection Service and for which the Inspection Service had found no violation. The defendant asserts that for these same reasons, the principles of reasonableness and proportionality have been violated. In addition, the principle of reliance on the defendant was also violated. The principle of trust or the principle of legal certainty implies that "the right must be foreseeable and accessible so that the litigant can reasonably provide for the consequences of a given act at the time it is performed".3

free text carried out by the Translation Service of the General Secretariat of the Protection Authority data, in the absence of an official translation] Furthermore, the public authority cannot deviate from one

political line without

objective and reasonable justification, according to

there

respondent.4 The respondent further submits that the principle of equality and the principle of non-discrimination as set out in Articles 10 and 11 of the Constitution have also been violated. Indeed, it cannot reasonably be justified why the DPA is following up on the leak of

1 Art. 100. § 1. The litigation chamber has the power to:

1° dismiss the complaint without follow-up;

2° order the dismissal;

3° pronouncing the suspension of the pronouncement;

4° to propose a transaction;

5° issue warnings and reprimands;

6° order to comply with requests from the data subject to exercise these rights;

7° order that the person concerned be informed of the security problem;

8° order the freezing, limitation or temporary or permanent prohibition of processing;

9° order compliance of the processing;

10° order the rectification, restriction or erasure of the data and the notification thereof to the data recipients;

11° order the withdrawal of accreditation from certification bodies;

12° to issue periodic penalty payments;

13° to issue administrative fines;

14° order the suspension of cross-border data flows to another State or an international body;

15° forward the file to the public prosecutor's office in Brussels, who informs it of the follow-up given to the file.

2 Judgment of the Markets Court of September 2, 2020, 9.4.

3 I. OPDEBEEK and S. DE SOMER, “Hoofdstuk III - Beginselen van behoorlijk bestuur” in S. DE SOMER and I. OPDEBEEK (ed.), Algemeen bestuursrecht (second edition) - hardcover edition, 2nd edition, Brussels, Intersentia, 2019, p. 412-413.

4 I. OPDEBEEK and S. DE SOMER, “Hoofdstuk III - Beginselen van behoorlijk bestuur” in S. DE SOMER and I. OPDEBEEK (ed.), Algemeen bestuursrecht (second edition) - hardcover edition, 2nd edition, Brussels, Intersentia, 2019, p. 412-413.

data in this case, while similar data leaks by third parties do not

the subject of no sequel. The fact that, according to its evaluation criteria, the General Secretariat has

apparently decided at first that no follow-up was necessary and that the

notification of the data breach was only followed up several months later, at

the initiative of the Inspection Service, also shows that in

the present case, to

constellations of facts are equal, there can be no question of equal treatment.

20. In this regard, the Litigation Division refers to Article 72 of the LCA, according to which

the Inspector General and the inspectors "may carry out any investigation, control and

any hearing, as well as collecting any information they deem useful in order to ensure that

the fundamental principles of the protection of personal data, in the

framework of this law and the laws containing provisions relating to the protection of the

processing of personal data, are effectively respected".

21. In view of the foregoing, it is up to the Inspection Service, within the framework of the

powers conferred on him, to take any investigative measures he deems necessary. There

The Litigation Chamber itself, as an administrative litigation body, must establish

its decisions on investigative actions that clearly fall within the legal framework within

which the administrative bodies must act.5 In the present case, there is no reason

to call into question the legality of the investigative acts of the Inspection Service.

II.2. Article 5, paragraph 1, a), c) and f) and paragraph 2, article 6, paragraph 1, article 24,

paragraph 1 and article 25, paragraphs 1 and 2 of the GDPR

22. In its capacity as data controller, the defendant is bound to respect the

data protection principles and must be able to demonstrate that these are

complied with (principle of responsibility – Article 5, paragraph 2 of the GDPR).

23. It must also, also in its capacity as controller, take all necessary

measures necessary to ensure and be able to demonstrate that the processing is carried out

in accordance with the GDPR (Articles 24 and 25 of the GDPR).

24. The Litigation Chamber recalls the principle of Article 5, paragraph 1, a) of the GDPR which

provides that personal data may only be processed lawfully.

This means that there must be a legal basis for the processing of personal data

personal, as referred to in Article 6(1) GDPR. To flesh out this principle of

5 by analogy with the judgment of the Court of Appeal of Brussels (Cour des Marches) of July 7, 2021, p. 18: "As part of

discretionary powers, the principles of good administration allow the judge to examine whether the administration has

exercised the power conferred on him within the limits of legality. In this respect, the judge has only a marginal right of control.

The judge can only declare the behavior complained of wrongful if it goes against the opinions of any body

normally prudent and reasonable administrative. This is particularly the case when the decision is not based on

concrete data and would run counter to reasonableness, and that the administration would therefore commit

a manifest error of assessment. The principle of "reasonableness" limits discretion only by not tolerating

that what has been decided is manifestly disproportionate to the facts (including all the documents in the file)

on which the decision is based. [Free translation carried out by the translation service of the Authority for the protection of

data, in the absence of an official translation]

Decision on the merits 183/2022 - 8/19

basis, Article 6(1) of the GDPR provides that personal data shall not

can only be processed under one of the legal bases set out in this article.

Where personal data is processed, it must therefore be adequate

and relevant to the purpose. Furthermore, no more data can be processed at

personal character than what is necessary for the purpose (Article 5.1.c) of the GDPR).

Article 5.1.f) of the GDPR prescribes that personal data must be "processed

in such a way as to ensure appropriate security of personal data, including the

protection against unauthorized or unlawful processing and against loss, destruction or

accidental damage, using technical or organizational measures

appropriate".

25. With regard to the disputed processing, the Inspection Service notes in its report that in the context of the complaint in this case, the defendant committed a violation of Article 5, paragraph 1, a), c), f) and paragraph 2 of the GDPR, on the basis of the following elements:

•

the principle of legality has been violated because the sending of personal data of the complainant to a wrong addressee was not based on a legal basis such as referred to in Art. 6(1) GDPR;

•

•

the principle of data minimization was violated because the defendant processed more of the complainant's personal data than was necessary as a result of being sent to the wrong recipient;

the principle of integrity and confidentiality has been violated because by sending data of the complainant's personal nature to the wrong addressee, the defendant compromised the confidentiality of such personal data; And

• by sending the complainant's personal data to the wrong recipient, the defendant failed to take the technical and organizational arrangements necessary to ensure and be able to demonstrate that the processing was carried out in accordance with the GDPR.

26. Despite this violation of the aforementioned articles in the context of this case, the Service of Inspection observes that the defending party generally seeks to respect the obligations imposed by Article 5 of the GDPR. The Inspection Service observes, however, that this does not detract from the concrete violation mentioned above.

27. The Respondent acknowledges that the email dated June 2, 2021 was addressed to the Complainant, but that due to occasional human error, personal data relating to

to the complainant were inadvertently sent to a third party. She explains that this is due to

fact that the plaintiff's lawyer's email address is similar to another email address

in the defendant's messaging system. The defendant maintains that such

unintentional, unintentional action cannot give rise to a violation of the GDPR.

28. Respondent argues that it took all appropriate steps to comply

to its data protection obligations. So she took action

following, which are relevant in this case:

To. Drafting and deployment of a confidentiality and data protection policy

company-wide ("Group Compliance Rule Data Protection") which

clarifies GDPR requirements and their implementation for Group Y entities;

b. Classification system for internal and external emails (in categories

public, internal, confidential and strictly confidential);

vs. Setting up a warning message in the messaging system

the defendant's electronic mail when collaborators send an e-mail to

an external email address;

d. Encryption and password protection of external email attachments

whose content is (strictly) confidential;

e. Access control measures to the defendant's systems;

f. Measures regarding the masking of information in the internal systems of the

defendant;

g. In order to proactively inform departments of issues they need to

take into account, a "Compliance Checklist" has been deployed with a section

explicit for data protection;

h. Drafting and implementation of a "Health Data Framework", which includes the

Respondent's data processing policy and strategy

relating to health. This Health Data Framework is reviewed annually by

representatives of different functions (at risk) (Compliance (of which the DPO is

part), Legal, Risk, CC Privacy, indemnity policy, medical community, ...).

The Framework provides concrete guidelines and defines requirements for

the processing of medical data within Y Assurances, in particular (i)

rules concerning the communication of data relating to health and the use

secure communication channels, both internally and externally, (ii) rules

specific regarding the processing by third parties, external parties and (iii)

specific rules regarding the retention of health-related data;

i. In the field of Information Security, there is a comprehensive framework of standards for

group which directly or indirectly contain rules on the protection

Decision on the merits 183/2022 - 10/19

data and

confidentiality, such as what means of

communication can be used for what type of data;

d. Training and awareness: the defendant ensures that its employees

know how to process personal data appropriately

and secure. All employees must undergo basic training

Mandatory under GDPR. In addition, the defendant launched an online training

for all its employees who process health-related data.

This online training focuses in more detail on data processing

related to health and includes important parts such as guidelines

clear on the use of secure communication channels, among other things.

An update of this training has been made and the new version has been

implemented on January 24, 2022. Training sessions must be

be repeated at regular intervals. Participation in these trainings is subject to

recording and monitoring, and the knowledge acquired is then

verified by a mandatory test;

k. In addition to the mandatory training sessions, monthly communications on

various GDPR-related topics are published via the communication platform

internal "Y Connect";

I. In addition to internal governance procedures, several support services for the

breast of

the defendant provide daily advice and support

GDPR, including: (i) the central Competence Center Privacy

(hereinafter "CC Privacy") in the front line, (ii) supported by Compliance Risk

Managers (CORM) appointed in a decentralized manner in the front line and (iii) the

Group Compliance Data Protection Unit, of which the DPO of Y Assurances is a member,

in the second line.

29. The defendant argues that it prefers to communicate through more secure channels than

emails (like some applications), but this is not always possible.

This case concerns communications with a client's lawyer such that

e-mail was the only electronic communication channel available to the defendant.

Finally, the defendant stresses that it has made numerous efforts to mitigate this kind of

risks, but that human error will always remain a residual risk.

30. The Litigation Division draws attention to the fact that the presence or absence of an intention

does not constitute a criterion for the presence or not of a processing of personal data

personal within the meaning of Article 4, point 2) of the GDPR.6 Although it was not the intention of the

6 Article 4 of the GDPR: "For the purposes of this Regulation, the following terms mean:

[…]

defendant to send the e-mail to the third party, the mere fact that the e-mail was indeed sent to the

wrong recipient is enough to qualify this sending of treatment, which should be checked
legality.

31. As also acknowledged by the Respondent, the present case concerns a breach of
personal data. For all practical purposes, the Litigation Chamber recalls
that a personal data breach is a security breach resulting in,
accidentally or unlawfully, the destruction, loss, alteration, unauthorized disclosure
authorization of personal data transmitted, stored or processed from another
manner, or unauthorized access to such data. By sending the email to the wrong
recipient, this third party could also access this personal data from the
complainant. It is therefore a question of a breach of confidentiality, namely a
illicit or involuntary communication or access of/to personal data.
The personal data in question were in fact exposed involuntarily
for a (short) period to external persons, thus jeopardizing the
privacy.

32. The Litigation Division considers that all of the elements presented demonstrate that the
defendant cannot rely on any legal basis of Article 6(1)
of the GDPR demonstrating the lawfulness of the disputed data processing. Furthermore, the treatment
data has compromised confidentiality and integrity, as third parties may have taken
knowledge of these data.

33. Insofar as necessary, the Litigation Chamber also recalls that under
GDPR Article 9, sensitive data, such as health data
(in this case, the e-mail contained the fact that the person concerned had had an accident
resulted in injury), cannot in principle be treated. Given their nature
sensitive, the processing of special categories of personal data is done
therefore subject to a general ban on processing. The GDPR, however, formulates a
limited number of exceptions to this rule and these exceptions apply to all

special categories of personal data. For the sake of completeness, the House
Contentious emphasizes that none of these exceptions could be used for the
data processing in question.

34. In this respect, the Litigation Chamber considers that since the sending was an error, the intention
was not at all to send the e-mail to the wrong recipient, and that the defendant had
not foresee that such a dispatch would occur. This follows from the very nature of an error.

2) "processing" any operation or set of operations whether or not carried out using automated processes and
applied to personal data or sets of personal data, such as the collection, recording,
organization, structuring, storage, adaptation or modification, extraction, consultation, use,
communication by transmission, dissemination or any other form of making available, aggregation or
interconnection, limitation, erasure or destruction"

This is all the more true since, in the present case, there are no technical measures
or organizational to completely exclude the risk of an e-mail being sent
to the wrong recipient due to human error.

35. Although this personal data breach constitutes a violation of the
fundamental principles of Article 5(1) and Article 6(1) GDPR,
the Litigation Chamber finds that the defendant has taken the technical and
organizational arrangements necessary to comply with the fundamental principles of
Article 5, paragraph 1 and demonstrate it. It also emerges from the Inspection report that the
respondent generally complies with the obligations imposed by Articles 5, 24,
paragraph 1 and 25, paragraphs 1 and 2, of the GDPR. In this case, the disputed processing concerns
human error, the risk of which is never totally non-existent.

36. In a non-exhaustive list of measures that controllers can
take to respect the principle of responsibility, the Group 29 refers in its Lines
guidelines on personal data breach notification under the

Regulation 2016/6797, among others, to the following measures to be taken: the implementation and monitoring control procedures to ensure that all measures do not exist not just on paper but are also executed and function in the practice, the establishment of internal procedures, the development of a written policy and binding in terms of data protection, the development of procedures internal for management and effective notification of breaches of Security.

The documents show that the defendant regularly carries out actions of awareness and that staff are also aware of the basic principles and obligations of controllers under the GDPR. In this way, the risk residual of such personal data breaches is kept to a minimum.

37. Consequently, the Litigation Chamber considers that there is a question of a violation of Articles 5, paragraph 1, a), c) and f) and paragraph 2, Article 6, paragraph 1, Article 24, paragraph 1 and Article 25, paragraphs 1 and 2, but that this does not require imposing a fine or corrective action and that it is appropriate to order a waiver of lawsuits. In this regard, the Litigation Division refers to the fact that the defendant has took the necessary steps to get the wrong recipient to delete the email as well as the fact that the violation is not the result of a structural problem and that sufficient proactive measures are in place to ensure GDPR compliance.

7 Guidelines on Personal Data Breach Notification under Regulation (EU) 2016/679, wp250rev01, Article 29 Working Party.

II.3. GDPR Article 33 and GDPR Article 34

II.3.1. Article 33 GDPR

38. When such a personal data breach occurs, the GDPR requires the
controller to notify the competent national supervisory authority and,
in certain cases, to communicate this violation to the persons whose data to
personal character are affected by this violation.

39. With regard to notification of a personal data breach to
the supervisory authority, the Litigation Chamber refers to Article 33 of the GDPR which provides
that "In the event of a personal data breach, the data controller in
notify the violation in question to the competent supervisory authority in accordance with Article
55, as soon as possible and, if possible, 72 hours at the latest after taking
knowledge, unless the violation in question is not likely to cause a
risk to the rights and freedoms of natural persons. When the notification to the authority
control does not take place within 72 hours, it is accompanied by the reasons for the delay."

40. The Inspection Service concluded in its report that notification of the breach to the DPA
and to the persons concerned was not made in due time, on the basis of the findings
following. The breach occurred on June 2, 2022, the internal notification of the breach of
personal data by the employee concerned to the Data Protection Unit of the
defendant took place on June 4, 2022. The notification of the data breach
personnel at the APD took place on June 7, 2022. This notification therefore took place more than 72 hours
after the discovery of the personal data breach, which constitutes a
violation of Article 33 of the GDPR, according to the inspection report.

41. The defendant contests these findings. She maintains that the notification to the DPA had
place in due time. The defendant argues that the report does not show that the Service
d'Inspection has sufficiently investigated the moment when the moment of taking
of knowledge. Contrary to the inspection report, the defendant argues that the
starting point of this period is not the moment when the breach actually occurred,
but the moment when the data controller has been informed of a possible violation

and after having actually found that it was a reportable incident. The lines

Article 29 Working Party guidelines on data breach notification to

personal character pursuant to Regulation (EU) 2016/6798 provide that

"The exact moment at which a data controller can be considered to have taken

"knowledge" of a specific breach will depend on the circumstances of the breach in

8 Guidelines on Personal Data Breach Notification under Regulation (EU)

2016/679, wp250rev01, Article 29 Working Party, p. 11-14.

question".9 According to the Article 29 Working Party, a data controller took

knowledge "After having been informed of a possible violation by an individual, by a

media organization or by another source, or when he himself has detected a

security incident, the data controller may conduct a brief investigation in order to

determine whether a violation has actually occurred."10 Indeed, it may take some

time to determine whether personal data is actually

compromised: "This short period allows the controller to open a

investigation and to collect evidence and other relevant data", according to

there

defendant. Referring to these Article 29 Working Party Guidelines, the

defendant asserts that the starting point of the 72-hour period referred to in Article 33

of the GDPR in this case begins to run when the defendant took

knowledge that the incident concerned personal data which

actually had to be notified, after all

THE

information required

concerning the incident have been communicated by the employee concerned to the department

competent internally (Data Protection Unit) (i.e. June 7, 2021 at 3:38 p.m.) and after a

analysis has actually established that the incident should be reported.

42. As explained above, the Litigation Chamber recalls that Article 33 of the GDPR provides that in the event of a personal data breach, the data controller processing notifies the personal data breach as soon as possible and, if possible, 72 hours at the latest after becoming aware of it. Thus, the starting point calculation of the 72-hour period begins when the defendant, as controller, has taken cognizance thereof.

43. The question then arises as to when a data controller can be considered to have "awareness" of a violation.

44. Based on the notification of the personal data breach by the respondent to the APD, the Litigation Chamber finds that an employee of the defendant sent the email in question to the wrong recipient on June 2, 2021 at 5:16 p.m. In the notification form, the data protection officer indicates that the collaborator discovered this error following an automatic response from the recipient. He has then sent the email to the correct recipient on June 2, 2021 at 5:24 p.m. Both emails were appended to the file. In the notification of the personal data breach staff at the DPA, the moment when the defendant became aware of the breach of personal data is set for June 2, 2021 at 5:24 p.m.

9 Guidelines on Personal Data Breach Notification under Regulation (EU) 2016/679, wp250rev01, Article 29 Working Party, p. 12.

10 Guidelines on Personal Data Breach Notification under Regulation (EU) 2016/679, wp250rev01, Article 29 Working Party, p. 13.

45. As explained above, the Respondent argues in its pleadings that the time limit for 72 hours only started to run when the Data Protection Unit received all the relevant documents of the employee concerned in order to carry out an analysis and after

that it has determined, as a result of this analysis, that this is indeed a reportable incident.

In this context, the Litigation Chamber refers to the EDPB Guidelines 9/2022

on notifications of personal data breaches. European Data

Protection Board (hereafter: EDPB)11 indicates that a data controller

shall be deemed to have taken "knowledge" when he has a reasonable degree of certainty that a

security incident has occurred leading to the compromise of personal data

staff. This must be assessed taking into account the circumstances of the breach

specific. In these Guidelines, the EDPB cites a few situations to illustrate when

there is a reasonable degree of certainty that a Security Incident has occurred, such as

example

the following

: "A third

informs a data controller that he has

accidentally received the personal data of one of its customers and provides the

evidence of such unauthorized disclosure. Once the controller has received

clear evidence of a breach of confidentiality, there is no doubt that it

took “knowledge” of it”.

46. The Litigation Chamber considers that in this case, the above example of the EDPB is very

similar to the facts of this case. Since the wrong recipient informed

the attorney for the complainant of the personal data breach, who has in his

had informed the defendant, there was therefore a reasonable degree of certainty that such

security incident had occurred. The EDPB recognizes the possibility for a person responsible for the

processing to conduct a brief investigation to determine whether a breach has in fact occurred

produced. During this investigation period, the controller may not be

considered to have taken "knowledge".12 Also in

the situation that

there

defendant refers in its submissions to the e-mail address of the plaintiff's lawyer (and,

moreover, the fact that the collaborator apparently discovered this error himself following

an automatic response from the wrong recipient) made it possible to quickly obtain a degree

reasonable certainty that a personal data breach has occurred, and

that the defendant was therefore aware of it.

47. As soon as the data controller has thus become "aware" of a security incident,

a reportable breach must be notified to the supervisory authority without unreasonable delay

and, if possible, within 72 hours if the personal data breach is

likely to pose a risk to the rights and freedoms of natural persons.

11 EDPB Guidelines 9/2022 on personal data breach notification under GDPR, of October 10, 2020, to be consulted via

https://edpb.europa.eu/system/files/2022-

10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf

12 EDPB Guidelines 9/2022 on personal data breach notification under GDPR, of October 10, 2020, p. 12.

During this period, the controller must assess this probable risk for

persons in order to determine whether the notification obligation actually applies and

what action(s) is (are) necessary to remedy the breach.13

48.

Only the short period which the controller may have needed to assess whether

this incident constituted a data breach is not included in the 72 hour time frame

(but since there was already a reasonable degree of certainty here already, this

period should therefore have been particularly short or almost non-existent in this case).

This 72-hour period is certainly intended to give the data controller the time

perform a risk analysis and assess whether a notification should be made to the DPA.

Contrary to what the defendant maintains, this period for carrying out this analysis

of risks is well and truly included in the 72-hour period.

49. This personal data breach was only reported to the Data Protection Unit by the employee concerned only in the afternoon of Friday June 4, 2021. After the Data Protection Unit has been notified, a risk analysis has been carried out and it has been decided to notify this personal data breach to the DPA. This notification had place on Monday, June 7, 2021 at 9:17 p.m. As the internal incident log also indicates, this notification took place outside the period of 72 hours after taking knowledge of the incident (which can be located on June 2, 2021). The explanation mentioned was that the employee concerned had belatedly informed the Data Protection Officer data. Following this, and at the request of the Data Protection Unit of the defendant, a further awareness-raising action has been undertaken in this regard. In view of the above, the Litigation Chamber concludes that the late notification of the data leak to the APD constitutes a violation of Article 33 of the GDPR. In view of the measures taken following this data leak, the Litigation Chamber concludes that a reprimand is appropriate. In view of the specific circumstances of this case, the imposition of a fine or of a correctional measure would be disproportionate.

II.3.2. GDPR Article 34

50. In accordance with Article 34 of the GDPR, the controller must in certain cases not only notify a violation to the supervisory authority, but also communicate it to people affected by it. This is the case when a breach is likely to involve a high risk to the rights and freedoms of natural persons.

51. The threshold for the communication of a violation to the persons concerned is therefore more higher than that for communication to the supervisory authorities and therefore all violations

13 EDPB Guidelines 9/2022 on personal data breach notification under GDPR, of October 10, 2020, p. 12.

which are notified to the supervisory authority must not be communicated to persons

concerned.

52. Article 34 of the GDPR provides that "[w]here a breach of personal data
is likely to create a high risk for the rights and freedoms of a person
physical", the data controller communicates the data breach
personnel to the person(s) concerned as soon as possible. Bedroom
Litigation observes that there is no 72-hour time limit set for notifying the
persons concerned. This notification must be made without delay, because the principal
purpose of notifying individuals is to provide them with specific information about
what steps they should take to protect themselves.14

53. In its notification of the data leak to the APD, the defendant indicated that the
person concerned would be informed because the loss of control of the personal data
personal data subject by dissemination that goes beyond what is necessary
poses a high risk to the rights and freedoms of the data subject. As already
explained above, the Data Protection Unit has received all the necessary documentation from the
employee concerned on June 7, 2021 at 3:38 p.m. The Data Protection Unit was then able to analyze
whether the data breach would involve a high risk to the complainant's rights and freedoms.
The complainant was then notified of the data breach the following day.

54. The Litigation Chamber notes that the data leak took place on June 2, 2021 and that the
complainant was only informed of this on June 8, 2021. This is because the employee
concerned did not inform the Data Protection Unit of the data leak in time, which
prevented it from carrying out a timely analysis of its impact on the rights and
complainant's freedoms. Given the foregoing, the Litigation Chamber concludes that there is
violation of Article 34 of the GDPR. The Litigation Chamber notes again that the
defendant took awareness-raising measures following this data leak and that the
Data Protection Unit performed the analysis required under Article 34 of the GDPR on
day after receipt of the necessary documents. Therefore, the House

Litigation concludes that a reprimand is appropriate, given the concrete circumstances

of this case.

II.4. Article 38(1) and Article 39 GDPR

55. The GDPR recognizes that the Data Protection Officer is a key figure in relation to

concerns the protection of personal data, including the designation, position

and missions are subject to rules. These rules help the controller to

14 See also recital 86.

fulfill its obligations under the GDPR but also help the data protection officer

data to carry out its tasks correctly.

56. Article 38(1) of the GDPR requires the controller to ensure that

the Data Protection Officer is involved, in an appropriate and timely manner

useful for all questions relating to the protection of personal data.

The involvement of the data protection officer should help ensure that he can

effectively perform the tasks mentioned in Article 39 of the GDPR.

57. After investigation, the Inspection Service concluded that no violation of Article 38,

paragraph 1 and Article 39 of the GDPR could not be ascertained. Based on the parts of the

file and the conclusions of the defendant, the Litigation Chamber considers that there is

no reason to take a different position in this respect.

III. Publication of the decision

58. Given the importance of transparency regarding the decision-making process of the Chamber

Litigation, this decision is published on the website of the Protection Authority

Datas. However, it is not necessary for this purpose that the identification data

of the parties are communicated directly.

FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation:

- to order a dismissal, under article 100, § 2 of the LCA, following the violations

oh

of Article 5, paragraph 1, c) and f) and paragraph 2, of Article 6, paragraph 1,

Article 24(1) and Article 25(1) and (2) GDPR;

- to formulate a reprimand, pursuant to Article 100, § 5 of the LCA, following the violation

o Articles 33 and 34 of the GDPR.

Pursuant to Article 108, § 1 of the LCA, this decision may be appealed to the

Court of Markets (Brussels Court of Appeal) within thirty days of its

notification, with the Data Protection Authority as defendant.

Decision on the merits 183/2022 - 19/19

Such an appeal may be lodged by means of a contradictory request which must include the

particulars listed in article 1034ter of the Judicial Code15. The contradictory request must be

filed with the registry of the Markets Court in accordance with article 1034quinquies of the Code

court, or via the e-Deposit computer system of Justice (article 3216ter of the Judicial Code).

(Sr.) Hielke HIJMANS

President of the Litigation Chamber

15 The request contains on pain of nullity:

the indication of the day, month and year;

1°

2° the surname, first name, domicile of the applicant, as well as, where applicable, his qualities and his national register

number or

Business Number ;

3° the surname, first name, domicile and, where applicable, the capacity of the person to be summoned;

4° the object and the summary statement of the means of the request;

5° the indication of the judge who is seized of the application;

6° the signature of the applicant or his lawyer.

16 The request, accompanied by its appendix, is sent, in as many copies as there are parties involved, by letter recommended to the court clerk or filed with the court office.