Dispute room

Decision on the merits 129/2022 of 23 August 2022

File number : DOS-2020-01079

Subject : Complaint for not providing an adequate level of security in the framework

of the processing of personal data.

The Disputes Chamber of the Data Protection Authority, composed of Mr Hielke Hijmans,

chairman and Messrs Dirk Van Der Kelen and Jelle Stassijns, members;

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

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

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

Data Protection Regulation), hereinafter GDPR;

In view of the law of 3 December 2017 establishing the Data Protection Authority, hereinafter WOG;

Having regard to the internal rules of procedure, as approved by the House of Representatives

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

Having regard to the documents in the file;

has made the following decision regarding:

The complainant:

Mr X, hereinafter referred to as “the complainant”;

The defendant:

Y, hereinafter referred to as “the defendant”.

I. Facts and procedure

1. On April 3, 2020, the complainant lodged a complaint with the Data Protection Authority against

defendant.

2. The complaint concerns the automatic provision of the complainant's personal documents

to a third. The complainant is co-housing with a friend, a third party in these proceedings. In the

In the context of this co-housing, it was agreed between the complainant and the third party that this third party

common water bill, in the name of the complainant, to his personal Y-

account. Y is a platform on which a user can manage his administration, such as a digital

archive. Here the user can upload and manage personal documents, such as invoices,

making payments, etc. Uploading the water invoice in the name of the complainant resulted in

that Y automatically suggested to the third party that other documents in the name of the complainant of

add other companies of which the complainant is a customer to the third party's account. This one

proposed new connections were rejected by the third party. At the request of the

First line service, the complainant contacted the defendant. The defendant stated

willing to resolve this issue. The complainant lodged a complaint against the situation as

it was before the technical adjustments to Y as made by the defendant.

3. On April 30, 2020, the complaint will be declared admissible by the Frontline Service on the basis of the

Articles 58 and 60 of the WOG and the complaint pursuant to Article 62, § 1 of the WOG is forwarded to the

Dispute room.

4. On August 11, 2020, the concerned parties will be notified by registered mail

of the provisions as stated in Article 95, § 2, as well as those in Article 98 WOG. Also

they are, pursuant to Article 99 WOG

informed of the deadlines to

to file defences.

The deadline for receipt of the defendant's statement of defense was thereby set

laid down on October 13, 2020, this for the conclusion of the complainant's reply on November 3

2020 and this for the defendant's reply on 24 November 2020.

5. On August 12, 2020, the defendant electronically accepts all communications regarding the case.

6. On August 17, 2020, the complainant electronically accepts all communication regarding the case.

7. On October 7, 2020, the Disputes Chamber will receive the statement of defense from the

defendant. The defendant emphasizes that a user account with Y is personal, whereby the

the intention is that a user only attaches documents in his or her name to his or her own account

adds. Since the third party uploaded the water invoice (in the name of the complainant),

proposed by Y two new compounds. The defendant explains that these connections

can be thought of as a folder in which documents are kept for a

end user of a particular company. This folder is only filled with documents and information

Decision on the merits 129/2022 - 3/9

when a connection is established with that company. When these two connections meet the third

were proposed, so there was no access to the documents themselves. The third could be based on

from these new proposals that the complainant was a customer of these two companies. Thereafter

the defendant emphasizes that the incident was resolved within 48 hours. Finally, the defendant argues

some improvement proposals to be implemented within six months

be in the platform:

- Better information about the effects of adding a connection;

- Better information about the personal nature of the user account.

8. On 9 October 2020, the Disputes Chamber will receive the statement of reply from the complainant. the complainant

refers to the respondent's statement of defense stating that a Y account

is personal. The complainant points out that he does not have an account and that he therefore believes that this is irrelevant

is. The complainant then argues that the Y platform is afflicted with some fundamental and illegal

construction errors. After all, the third party could enter an invoice in the name of the complainant, which

also has the effect of proposing new compounds, making the third

would have access to further personal data of the complainant. The complainant was also not

informed, consulted or warned about this in any way. The complainant emphasizes

also that the documents of the new connections were not added to the Y account of

the third party, but that the third party has formally stated that it has been made available to him for inspection

to be. The prevention of access to the documents is therefore due to the good intentions of

the third party and not by the necessary security measures of the platform, according to the complainant.

9. On November 24, 2020, the Disputes Chamber will receive the statement of reply from the defendant.

The defendant emphasizes that the personal nature of the user account is relevant

because of the combination of measures that Y takes and the functionalities that Y offers. It

correct use of Y is after all not to add other people's documents to one's own account.

The defendant then emphasizes that there are no fundamental and illegal construction errors in the

platform are present. According to the defendant, this complaint is the result of an agreement between

the complainant and the third. The complainant has given his consent to the third party to pay the water invoice,

in the name of the complainant, to be added to the user account of the third party on Y. To do this

document, the third party has had access to the complainant's personal data,

namely his customer number and security code on the invoice from his water supplier. Without

this data the third party could not add the invoice to his user account. The defendant

emphasizes that communication between

supplier and customer, such as invoices or other

confidential communications is beyond Y's control. The defendant has no access to

that data and has no influence on the way in which the supplier and the customer use this

handle data.

10. The complainant indicated in his conclusions that he was not informed or warned that (new)

connections would be made. The defendant points out in its claims that the complainant

is not a user of Y, as a result of which the defendant did not have his personal data to

to notify the complainant. Finally, the defendant wishes to refute that the third party had access

in the documents in the new connections mentioned above. The defendant argues that

the documents are only visible to a user when he has added them via the

entering a security code or accepting an invitation. Without this code or

invitation, no documents are added to a user's account and

no access to documents. Y's logs show that the third party accepted the invitation to new

did not accept the connection, so no documents were added and therefore

access is impossible. The defendant additionally states that it will adopt a constructive attitude and indicates:

to build in additional functionality within a period of six months, namely a

additional security with eID and/or Itsme. In this way, an additional check is made

created about the user's identity.

11. On May 25, 2022, the defendant will be notified that the hearing will take place on

June 21, 2022.

12. On June 21, 2022, the parties will be heard by the Disputes Chamber and will thus receive the

opportunity to present their arguments. The complainant appeared in person and the

defendant appeared through the CEO and his attorney. Subsequently, the case is

Dispute chamber under consideration.

13. On June 27, 2022, the minutes of the hearing shall be submitted to the parties in

in accordance with article 54 of the internal rules of the DPA. The parties

are hereby given the opportunity to have their comments, if any, added thereto as

annex to the official report, without this implying a reopening of the debates.

14. On 4 July 2022, the Disputes Chamber will receive some comments from the complainant with

with regard to the official report which it decides to include in its deliberations.

15. On July 5, 2022, the Disputes Chamber will receive the notification from the defendant

no

to formulate comments with regard to the official report.

16. On July 6, 2022, the Disputes Chamber notified the defendant of its intention to

to proceed with the imposition of an administrative fine, as well as the amount thereof

in order to give the defendant an opportunity to defend himself before the sanction takes effect

is imposed.

17. On July 12, 2022, the Disputes Chamber will receive the defendant's response to the intention to

the imposition of an administrative fine, as well as the amount thereof. The defendant

does not wish to comment on this.

II. Justification

Decision on the merits 129/2022 - 5/9

Article 5, 1 f) of the GDPR, Article 5, paragraph 2 of the GDPR, Article 24, paragraph 1 of the GDPR and Article 32, paragraph

1 and paragraph 2 of the GDPR regarding identity verification

18. Article 5, 1, f) of the GDPR requires that "[personal data] by taking appropriate

technical or organizational measures are processed in such a way that a

appropriate security is ensured, and that they are protected, inter alia, against

unauthorized or unlawful processing and against accidental loss, destruction or

damage".

19. Further elaborating on Article 5(1)(f) GDPR, Article 32(1) GDPR states that the defendant as

controller must take appropriate technical and organizational measures

to ensure a level of security appropriate to the risk. This must take into account

are taken into account the state of the art, the implementation costs, as well as the nature,

scope, context, processing purposes and likelihood and seriousness of the

various risks to the rights and freedoms of individuals.

20. Article 32(1) of the GDPR provides that when assessing the appropriate level of security

processing risks must be taken into account, especially as a result of destruction,

the loss, alteration, unauthorized disclosure of or access to

data transmitted, stored or otherwise processed, either accidentally or

unlawful.

21. The Disputes Chamber points out that accountability

pursuant to the articles

5 (2) GDPR, Article 24 GDPR and Article 32 (1) and (2) GDPR entails that the

controller takes the necessary technical and organizational measures,

in order to ensure that the processing is in accordance with the GDPR. This obligation

belongs to the accountability of the defendant pursuant to Article 5, paragraph 2 GDPR, Article 24 GDPR

and Article 32 GDPR. The Disputes Chamber points out that the accountability obligation of Article 5, paragraph 2

GDPR and Article 24 GDPR is one of the central pillars of the GDPR. This means that on the

controller has an obligation, on the one hand, to take proactive

measures to ensure compliance with the requirements of the GDPR and, on the other hand,

being able to demonstrate that he has taken such measures.

22. The first step to ensure the appropriate level of security for the processing of personal data

determining is to map out the risks of that processing and to weigh them up.

Based on this, it must be determined which measures are necessary to ensure adequate security

against these risks. It follows from the GDPR that when weighing up the

data security risks due attention should be paid to risks that arise

may arise during personal data processing, such as unauthorized disclosure of or

Decision on the substance 129/2022 - 6/9

unauthorized access to processed data. When inventorying and assessing the

risks are mainly relevant to the consequences that persons may experience from an unlawful

processing of personal data. The more sensitive the data is, or the more

context in which they are used a greater threat to privacy

mean, stricter requirements are imposed on the security of personal data.

23. As already mentioned above, platform Y is a platform on which a user is

administration, comparable to a digital archive. Hereby the user can

personal documents, such as invoices, upload and manage, make payments, etc. From the

the defendant's conclusions, the Disputes Chamber understands that an account on the platform is

a user is created and also managed in his name (or that of family members). The

user can designate companies (suppliers) whose administration he wishes to receive

and, provided that you have completed the necessary steps, add it to his account. Given the nature of the

companies with which the controller works and the large number of suppliers

that uses Y, the Disputes Chamber determines that personal data of users of

widely shared across the platform, and that it (mostly) involves sensitive data, such as

data is processed by, among others, banks and mutual insurance companies. The sensitive nature of this

data must be included in the aforementioned consideration of the risks that the

security level should be adjusted accordingly.

24. The Disputes Chamber understands from the defendant's claims that the use of Y

in principle it is not the intention to send invoices in someone else's name in a personal

add user account. To this end, the defendant provides a security code that must be

entered when adding the invoice to the account. The Disputes Chamber states

notes, however, that the defendant itself argues in its claims that it has no control over the

communication between the supplier and the customer and what happens with this communication. This brings

This means that in the event of loss or improper use of the aforementioned security code, the

Defendant has no way of verifying whether this code is lawfully used

is becoming.

25. The Disputes Chamber is therefore of the opinion that the defendant has not taken the sufficient security measures

has provided, so that even in the event of loss or improper use of the aforementioned communication between

the supplier and the customer, the customer's personal data remains secure. As above

has already been mentioned, in that case a third party may, due to improper use, receive various financial and

consult the data subject's medical data, which may not be the intention. Moreover,

the Disputes Chamber determines, it is possible that by adding one invoice

several new connections are established automatically. Performing a

verifying the identity of the person using the security code would prevent

documents would be added to the account of the wrong data subjects.

Consequently, the Disputes Chamber states that additional verification offers a more secure solution.

26. The Disputes Chamber refers to the summary conclusion of the defendant in which it states that it

wish to improve the functioning of their platform, based on the complainant's comments. So

would they intend to take initiatives within six months to

better inform those involved about the effects of adding a compound

on the one hand and on the personal nature of the user account on the other.

27. The defendant also indicates that, within a period of six months, additional security will be provided, by means of

provide two-step verification through an identification via e-ID or Itsme whereby the

the person concerned can confirm that he indeed wishes to add those invoices to his account.

28. During the hearing, the defendant explains the concrete steps taken with

regarding the taking of technical and organizational measures in the context of the

establishing an appropriate level of security with a view to protecting

personal data.

29. The defendant explains that 3 improvements were made following the complaint:

a. The user is better informed about the account and its personal nature,

as well as the security code and its personal use;

b. The user is better informed about the origin of the connections and the

consequences thereof; and

c. An additional validation via two-factor bank account verification has been implemented

to ensure the identity of the correct data subject.

In addition, the defendant argues that no more new connections are proposed.

30. The Disputes Chamber notes that, although the defendant has at present applied the additional two-factor

authentication, there was previously an insufficient level of security when establishing

coming of connections. In this context, the Disputes Chamber refers to the sensitive

character of the data that was insufficiently secured. The Disputes Chamber also holds

take into account the fact that the defendant will do so soon after reporting the security problem

has remedied.

31. In view of the above, the Disputes Chamber is of the opinion that there has been an infringement of

Article 5 (1) f) GDPR, Article 5 (2) GDPR, Article 24 (1) GDPR and Article 32 (1) and (2) GDPR

since, on the one hand, the defendant did not have sufficient technical and organizational measures

taken to ensure a level of security appropriate to the risk and, on the other hand, they

determining the appropriate security risks has not sufficiently taken into account the

processing risks, in particular in the event of loss or unauthorized use.

Decision on the merits 129/2022 - 8/9

III. Sanctions

32. The Disputes Chamber considers the infringement of Article 5, paragraph 1, f), Article 5, paragraph 2, Article 24, paragraph

Article 32(1) and (2) GDPR, as the defendant did not take sufficient precautions to

prevent potential data leaks.

33. The Disputes Chamber considers it appropriate to impose an administrative fine amounting to

of EUR 2,500 (Article 83, paragraph 2, Article 100, §1, 13° WOG and Article 101 WOG).

34. Taking into account Article 83 GDPR and the case law1 of the Marktenhof, the motivation

Dispute chamber imposing an administrative sanction in concrete terms:

a. The seriousness of the infringement — it is the lack of appropriate technical and

organizational measures to ensure a level of security appropriate to the risk

guarantees by a company whose core activity is the processing of (sensitive)

constitutes personal data;

b. The duration of the infringement — the infringement was not noticed by the defendant itself, but

after a complaint about this, the problem was quickly resolved;

c. The solution of the infringement – the defendant has shown constructive

attitude and was able to remedy the infringement within a short period of time.

35. The whole of the elements set out above justifies an effective,

proportionate and dissuasive sanction as referred to in Article 83 GDPR, taking into account the

certain assessment criteria. The Disputes Chamber points out that the other criteria of art.

83, para. 2 GDPR in this case are not of a nature that they lead to a different administrative fine

than that determined by the Disputes Chamber in the context of this decision.

36. Superfluously, the Disputes Chamber also refers to the guidelines regarding the calculation of

administrative fines (Guidelines 04/2022 on the calculation of administrative fines under the

GDPR) which the EDPB published on its website on May 16, 2022, for consultation. Since

these guidelines are not yet final, the Disputes Chamber has decided not to

to be taken into account in determining the amount of the fine in the present proceedings.

37. The facts, circumstances and established infringements therefore justify a fine whereby

the defendant is sanctioned, so that practices involving such infringements would not

are repeated.

IV. Publication of the decision

1 Brussels Court of Appeal (Market Court section), X t. GBA, Judgment 2020/1471 of 19 February 2020.

Decision on the merits 129/2022 - 9/9

38. Given the importance of transparency in the decision-making of the

Dispute room, becomes

this one

decision

published

on

the website

from

the

Data Protection Authority. However, it is not necessary that the identification data

of the parties be published directly.

FOR THESE REASONS,

the Disputes Chamber of the Data Protection Authority decides, after deliberation, to:

- Pursuant to Article 83 GDPR and Articles 100, 1, 13° and 101 WOG, an administrative fine of

EUR 2,500 to be imposed on the defendant for the infringements of Article 5.1.f, Article 5.2, Article 24,

paragraph 1 and article 32, paragraphs 1 and 2 GDPR;

Against this decision, pursuant to art. 108, § 1 WOG, appeal must be lodged within a period

of thirty days, from the notification, to the Market Court, with the Data Protection Authority as

defendant.

Pursuant to Article 108, § 1 of the WOG, within a period of thirty days from the notification

appeal against this decision to the Marktenhof (Brussels Court of Appeal), with the

Data Protection Authority as Defendant.

Such an appeal may be lodged by means of an adversarial petition that the

1034ter of the Judicial Code must contain listed entries2. The petition on

contradiction must be submitted to the registry of the Market Court in accordance with Article

1034quinquies of the Ger.W.3, or via the e-Deposit IT system of Justice (Article 32ter of

the Ger.W.).

(get). Hielke Hijmans

Chairman of the Disputes Chamber

2 The petition states on pain of nullity:

1° the day, month and year;

2° the surname, first name, place of residence of the applicant and, where applicable, his capacity and his national register or

company number;

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

4° the subject matter and the brief summary of the grounds of the claim;

5° the court before whom the claim is brought;

6° the signature of the applicant or of his lawyer.

3 The application with its annex is sent by registered letter, in as many copies as there are parties involved, to

the clerk of the court or at the registry.