Dispute room

Decision on the merits 101/2022 of 3 June 2022

File number : DOS-2019-04867

Subject: complaint because of assigning the complainant's telephone number to a third party

The Dispute Chamber of the Data Protection Authority, composed of Mr Hielke

Hijmans, chairman and Messrs Dirk Van Der Kelen and Yves Poullet.

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

in connection with 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;

In view of the

rules of

internal order, as approved by the Chamber of

Representatives on 20 December 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, represented by Mr. B. Bruyndonckx and Mr. L. Kuyken, both

with offices at Havenlaan 86c b113, 1000 Brussels. hereinafter “the

defendant"□

.□

.□

.□

.□

.□

.□

Decision on the merits 101/2022 - 2/29□

I. Facts and procedure□

Process sequence□

1.□

On January 22, 2021, the Disputes Chamber made decision 05/2021 against the defendant,□

where a fine of EUR 25,000 was imposed on the defendant for violations of the□

Articles 5.1.f, 5.2, 24, 32, 33.1 and 5, 34.1 GDPR.□

• On February 19, 2021, the defendant lodged an appeal against decision 05/2021 of the□

Dispute room.□

• On 20 May 2021, the Disputes Chamber withdrew its decision of 22 January by□

by means of withdrawal decision 61/2021 and thereby decides to reconsider the case□

will take by means of a new procedure on the merits.□

• On June 30, 2021, the Marktenhof ruled in the appeal lodged by Y.□

• On September 23, 2021, the Disputes Chamber sent the new conclusion calendar□

parties in order to initiate new proceedings on the merits.□

• On November 2, 2021, the Disputes Chamber received the statement of defense from the□

defendant.□

• On April 25, 2022, in accordance with Article 53 of the Rules of□

internal order of the Data Protection Authority heard by the Disputes Chamber.□

2.

This decision is made on the basis of a new procedure on the merits. The

The Disputes Chamber has made its primary decision 05/2021 following the complaint in

after all, this file has been withdrawn and has decided to initiate a new procedure

to the bottom. The present decision is therefore made on the basis of the complaint, the

filed defenses and the other relevant documents of the proceedings.

The complaint and the primary decision on the complaint by the Disputes Chamber

Decision on the merits 101/2022 - 3/29

3.

complainant

served

on

20

September

2019

a

complaint

to Y

in

Bee

the

Data Protection Authority. The complaint was declared admissible on 30 September 2019

by the Frontline Service. The complaint implied that the complainant's mobile telephone number was

provider Y would have been assigned to a third party, as a result of which the complainant could no longer access his number

possess. The complainant's SIM card was deactivated and the third party would therefore have knowledge

be able to record the complainant's personal GSM traffic and calls, as well as

linked accounts (such as Paypal, WhatsApp and Facebook) from September 16 to 19

2019.

4. On April 15, 2020, the Disputes Chamber decided that the complaint was ready for handling

on the merits and notified both the complainant and the defendant by registered mail of

this decision. The parties were also notified of the provisions set out in

Article 98 of the WOG and the time limits for submitting their defences. The deadline

for receipt of the statement of reply from the defendant was determined on May 27, 2020; the

deadline for receipt of the complainant's statement of reply is 17 June 2020 and the

final date for receipt of the defendant's reply statement on July 8, 2020. At 27

In May 2020, the defendant filed a statement of defense. On November 9, 2020,

the defendant, in accordance with Article 53 of the Rules of Internal Order, heard by the

Dispute room. The minutes of the hearing will be sent to the parties on November 19, 2020

submitted. On December 7, 2020, the intention is to impose a fine

transferred to the defendant. Respondent to this intention on December 22, 2020

responded extensively.

5.

Subsequently, the Disputes Chamber took decision 05/2021 on 22 January 2021 and the

imposed a fine of EUR 25,000 on the defendant for violation of Articles 5.1.f,

5.2, 24, 32, 33.1 and 5, 34.1 GDPR.

6. On 19 February 2021, Y appealed to the Marktenhof against the decision of the

Disputes Chamber of 22 January 2021. Y argued in the appeal that the Disputes Chamber

making the decision had disregarded the rights of defense and the principles of

good governance had been violated. Defendant

stated, among other things, that it

principle of proportionality was violated because the Disputes Chamber had no investigation

requested from the Inspectorate. According to the defendant, the Disputes Chamber also violated the

principle of reasoning and the principle of reasonableness, by a defendant,

disproportionate decision with a high fine. The defendant was of the opinion

that the rights of defense were violated by not giving the defendant a chance to

express views on the basis of a concrete indictment. The Dispute Room

according to the defendant, had wrongly come to the conclusion that there had been infringements

on Articles 5.1.f, 5.2, 24, 32, 33.1 and 5, as well as 34.1 GDPR.

Decision on the merits 101/2022 - 4/29

7.

Pending the appeal, the above decision was revoked by the Disputes Chamber

by the withdrawal decision 61/2021. In that decision, the Disputes Chamber considered as follows:

Whereas the Marktenhof in its rulings 2020/AR/813 of 18 November 2020 and

2021/AR/1159 of 24 February 2021 pointed out the importance of prioritizing data subjects

to inform the handling of the file of the exact allegations and/or infringements

what he might be guilty of; Whereas Y NV during the appeal to the

Marktenhof has argued against the decision on the merits 5/2021 of 22 January 2021 that it

the procedure preceding this decision has not been sufficiently informed about the exact

allegations and/or infringements.

Has decided to:

. the decision on the merits 5/2021 of 22 January 2021 against Y NV by means of the present

decision to withdraw.

. reopen the proceedings before the Disputes Chamber and the parties, subject to the

to request the submission of new means of defense specified in Article 98 of the GBA Act."

8.

No appeal was lodged by the defendant against the withdrawal decision of the Disputes Chamber

set. During the hearing of the appeal against the primary

decision of the Disputes Chamber, however, that the Marktenhof "Again justice and with

exercise of its fullness of jurisdiction, should assess the merits of the case

and to substitute its own decision for the Disputes Chamber."

9. On June 30, 2021, the Marktenhof ruled. In it, however, the court held as follows:

the above-mentioned request of the defendant:

Now that the decision of 19 May 2021 states that it has been decided "to open the procedure for the

To reopen the Dispute Chamber and the parties with due observance of the provisions of Article 98

of the GBA Act to submit new defenses" and no recourse against this

has been instituted, Y has agreed that the Marktenhof will not have its own

can make a decision and that, first of all, the Disputes Chamber must be given the opportunity to

proceeding."1

10. With the above, the Marktenhof has therefore confirmed that the decision of the

Dispute chamber against which an appeal was lodged by the defendant no longer exists in the

legal transactions and it is deemed never to have existed by the withdrawal decision. The

Defendant's claim that the Market Court, by virtue of its full jurisdiction, has its own

should make a decision by taking the place of the Disputes Chamber was by

the Marktenhof therefore declared it unfounded. The appeal is without purpose.

1 Recital 7.5 Marktenthof judgment

11. The Marktenhof also noted that the withdrawal of the decision cannot in itself

shall be regarded as proof that the Disputes Chamber has made a wrong or illegal decision

Has taken. According to the Marktenhof, there is also no question of any erroneous conduct on the basis of

of the Disputes Chamber. On the contrary, according to the Marktenhof, the withdrawal testifies to

respect for the principles of the rule of law by the Disputes Chamber.

New procedure on the merits

12. On September 23, 2021, the Disputes Chamber sent a new conclusion calendar to

parties. In this letter, the Disputes Chamber also summed up:

the charges against the defendant, which read as follows: "The defendant is charged"□

laid that:□

1. he has not carried out any, or has carried out an incomplete or incorrect verification when checking whether the□

third person who requested a migration of his SIM card from in the defendant's shop□

prepaid to postpaid and indicated that he is the holder of the telephone number actually□

that person was. As a result of the foregoing, his2 number was assigned to the third□

and could the third party have access to the telephone number and take cognizance of the□

the complainant's telephone traffic resulting in a data breach. Therefore, on□

defendant charged that he did not take the necessary technical and organizational measures□

would have taken in order to prevent a violation of the complainant's privacy (□

Articles 5.1.f, 5.2, 24 and 32 GDPR)□

2. he the data leak that has arisen as a result of the procedure described under 1□

has not reported to the Data Protection Authority nor to the data subject, in this case□

complainant (Articles 33.1, 33.5 and 34.1 GDPR)"□

13. The Disputes Chamber also formulated the following questions in order to provide greater clarity□

to obtain:□

"1. Has the defendant taken all necessary technical and organizational measures in accordance with the□

Articles 5.1.f, 24 and 32 GDPR and provided an appropriate level of security□

in order to prevent the -allegedly- allocating of the complainant's telephone number□

could happen to a third party and if so, can it demonstrate this?□

2. Can the defendant demonstrate that it has taken proactive measures in accordance with Article 5.2□

GDPR in order to ensure compliance with the provisions of the GDPR - including the above under 1□

mentioned measures- to guarantee ?□

2 This means the complainant's telephone number□

3. According to the respondent, was there a data breach, and in that case has the respondent□

complied with the duty to notify

to make use of that data breach at the

Data Protection Authority in accordance with Article 33.1 AVG and has these infringements

documented in accordance with Article 33.5 GDPR as well as notification thereof to the data subject

in accordance with article 34.1 of the GDPR?

14. The time limits for submitting defenses were set at:

- November 2, 2021 as the final date for receipt of the statement of reply from

defendant;

- 23 November 2021 as the final date for receipt of the complainant's reply;

-

14 December 2021 as the final date for receipt of the statement of reply from

defendant.

15. The Disputes Chamber received the statement of defense from the defendant on 2 November 2021

in which the following pleas are put forward:

• Defendant took all necessary technical and organizational measures in accordance with the

Articles 5 (1) (f), 24 and 32 of the GDPR and provided an appropriate level of security;

• Defendant took proactive measures in accordance with Article 5 (2) of the GDPR in order to

compliance with the requirements of the GDPR, including the technical and

to ensure organizational measures;

• Defendant acted in accordance with Articles 33 and 34 of the GDPR;

• According to the defendant, the Disputes Chamber will have to sit in a completely different

composition in view of the judgment of the Marktenhof in which this was determined. If the

composition of the Disputes Chamber in these proceedings would not differ completely

of the composition of the Disputes Chamber that ruled on January 22, 2021, is

the composition according to the defendant is irregular and the procedure equally so.

16. On April 25, 2022, the parties will be heard by the Disputes Chamber.

17. The minutes of the hearing will be sent to the parties on 9 May 2022.

18. On May 17, 2022, the Disputes Chamber will receive the comments from the defendant on the

police report. First of all, the defendant argues that the chairman Hielke Hijmans during the

hearing would have “admitted” that the decision of the Market Court which determined

that the Disputes Chamber must sit in a completely different composition if a case is a

second time by the Disputes Chamber, as is the case in this case, not by the

Litigation room would have been respected. The defendant is also of the opinion that the

does not adequately reflect verbally what the members would put forward during the session

to have. It does not specify what would be missing.

19. The sanction form was sent to the defendant on May 16, 2022.

20. On May 31, the Disputes Chamber will receive the respondent's response to the sanction form.

The content of the case

21. The complainant has been a customer of the defendant since 11 June 2015 and purchases (prepaid) mobile telephone servi

The complainant's telephone number is for the duration of four days, namely from 15 to 19

September 2019, awarded to a third party where the complainant's SIM card has been deactivated.

22. During these proceedings, the Disputes Chamber tried to gain insight into the course of

the events that led to the assignment of the complainant's telephone number to

a third. It becomes clear from this decision that a few things about the actual course

cannot be fully elucidated. According to the defendant, the third is on September 11, 2019 in one

of the defendant's stores in order to exchange the complainant's prepaid subscription

have it converted into a postpaid subscription with accompanying smartphone device that will be replaced after 24 months

subscription has been paid. According to the defendant, both the telephone number and the

SIM card number of the complainant provided by the third party. From September 11, 2019 changed

the complainant's subscription therefore changes from prepaid to postpaid. The third has its own

provided identification information that associated it with the postpaid

subscription so that all costs from then on were billed in the name of the third party.

However, the third did not yet have a SIM card attached to it on September 11, 2019.

the complainant's mobile number so that the complainant could continue to use the services himself

of the subscription. Four days later, on September 15, 2019, according to the defendant, the third

went to a Y-shop again and asked for a new SIM card attached to

the same mobile number. At that moment he got access to the mobile number of the

complainant and the complainant's SIM card was disconnected. The complainant was no longer in contact with the

network from then on.

23. The complainant describes in his complaint that he has been in contact with the defendant several times by telephone

and having been in the defendant's shops in order to be able to dispose of again

about his phone number. It was only on 19 September 2019 that the complainant was able to

have his phone number.

II. Justification

2.1 About the composition of the Disputes Chamber

24. The defendant expressly made reservations both at the conclusion and during the hearing

with regard to the composition of the Disputes Chamber. Defendant be there during the hearing

that the composition of the Disputes Chamber does not consist in its entirety of other physical persons

Decision on the merits 101/2022 - 8/29

existed and noted that the two members had been replaced while the chairman was in these proceedings

stayed seated. Moreover, in his response to the official report, the defendant stated that:

given that the chairman would have admitted not to the decision of the Market Court

to keep. The foregoing statement is incorrect. The Disputes Chamber will explain below with reasons

explain in detail why this composition of the Disputes Chamber was chosen at

the handling of this file.

25.

After all, the Marktenhof decided in its judgment of 30 June 2021 that the Disputes Chamber "in its

totality would have been composed by physical persons other than those who were part of

the Chamber when taking the currently contested decision." Defendant therefore argues that the

procedure is unlawful if the Disputes Chamber has not been constituted by three other parties

persons other than those who were part of the Dispute Chamber when taking the

primary decision.

26. The court further ruled that: "Although the members of the Disputes Chamber are not judges,

that this body would comply with the basic rules of good administration, including at least

give the appearance of impartiality".

27. The Disputes Chamber emphasizes that in this case there is no question of any

established illegality of the proceedings of the Disputes Chamber. From a judgment in which the

the impartiality of the Disputes Chamber is not at all questioned. It

the opposite is true. The Disputes Chamber has chosen to withdraw its first decision

with the motivation:

Whereas the Marktenhof in its rulings 2020/AR/813 of 18 November 2020 and

2021/AR/1159 of 24 February 2021 pointed out the importance of keeping data subjects

prior to processing the file about the exact allegations and/or

infringements of which he could be guilty; Whereas Y NV during the

has appealed to the Market Court against the decision on the merits 5/2021 of 22 January 2021

stated that it was insufficiently informed in the procedure preceding this decision

regarding the exact allegations and/or infringements."

28. There is no indication whatsoever that the Disputes Chamber - as it was first constituted - is biased

would be and could not (in part or even entirely the same composition) again

judge the case.

29. Against the

Moreover, the decision to withdraw from the Disputes Chamber did not become an appeal

registered by the defendant. Defendant requested the Marktenhof to make its own decision

to replace that of the Disputes Chamber and to rule on the merits of the

appeal lodged by it against the primary decision and which is pending

was withdrawn by the Disputes Chamber. The Market Court rejected the defendant's request

Decision on the merits 101/2022 - 9/29

occasionally, considering that due to the withdrawal decision of the Disputes Chamber, the contested

decision was deemed never to have existed in legal transactions. With that, the profession

become without object. The Court also noted that the withdrawal of the

decision in itself cannot be regarded as proof that the Disputes Chamber made a wrong decision

or made an illegal decision. The withdrawal of the decision testifies according to the

Market Court of respect for the principles of the rule of law by the Disputes Chamber.

30. In a judgment of 7 August 2018, the Marktenhof ruled in principle on the question whether a

case, after annulment due to a procedural defect, must be reassessed by a

differently composed body, or whether the body in the same composition is a new

may make a decision. It concerned a decision of the Belgian Competition Authority

(BMA). In this judgment, the Marktenhof ruled that a different composition in that case

was necessary, because Article IV.30 Code of Economic Law (WER) Article 828

Judicial Code (Ger. W.) applicable to the BMA. In article 828 Jud. W. are the

grounds for challenge for judges. Of crucial importance in that judgment was that it

Marktenhof ruled that Article 828 Ger. W. can only be applied to other persons

than the judges belonging to the judiciary if the law expressly so provides.

Since the WOG does not contain a provision that Article 828 Ger. W. declares applicable to the

members of the Disputes Chamber, members of the Disputes Chamber cannot

provision are challenged if they have previously taken cognizance of the same dispute.

31. The Disputes Chamber makes every effort

and does everything possible to make it

to observe the principle of impartiality as a general principle of good administration,

to ensure a fair trial for the parties. After all, this principle guarantees both

the personal impartiality of the members of the Dispute Chamber who make a decision,

as the structural impartiality of the Disputes Chamber in terms of its organisation,

the course of the procedure and the establishment of its decisions.3

32. However, according to settled case-law of the Council of State, the principle of impartiality is only

applies to the bodies of active management “to the extent that this is compatible with its own

nature, in particular the structure of the government”.4 The application of the principle may be more

certainly do not make it impossible to take a regular decision, namely

because this principle would make it impossible for the competent administrative authority to act.5 In

the extent that the application of the principle would result in, for example, a body being

could no longer exercise legal powers, the application of this principle

be pushed aside.

3 See, by analogy, Council of State 26 February 2015, no. 230.338, Deputation of the Antwerp Provincial Council, para. 10.

4 See eg RvS 3 October 2014, no. 228.633, ASBL Unsolicited Artists; December 10, 2020, no. 249,191, recital. 25.

33. The Disputes Chamber consists of a chairperson and six members, three of whom are Dutch-speaking and three

French-speaking.6 These members all have their own area of expertise. When treating a

file before the Disputes Chamber, the members are therefore involved on the basis of the language they use

speak and their expertise that is called upon. The principle of impartiality

applies as indicated above to the extent compatible with the nature and

government structure. The two Dutch-speaking members Frank De Smet and Jelle Stassijns

were sitting together with the chairman at the time of the primary handling of the complaint against

defendant. This means that only 1 Dutch-speaking member remains. It's for that reason alone

not possible for the Disputes Chamber to sit in a completely different composition

as this is simply incompatible with the nature and structure of the Litigation Chamber

and it would seriously impede the continuity of the Disputes Chamber. Since knowledge of

the language in which a complaint is handled before the Disputes Chamber is indispensable for a□

efficient way of handling, the members for the handling of a particular file□

initially appointed by the chairman – in accordance with Article 33 WOG and Article□

43 of the Rules of Internal Order - based on the spoken language and of course expertise□

on the relevant level. With regard to the language role, the basic principle is that - in addition to the chairman who□

meets the language requirements for all national languages – at least one member belongs to the language role of□

the language of the proceedings (and the other member has sufficient factual knowledge of the language).□

34. The Disputes Chamber recalls that the principle of good administration of impartiality□

according to legal doctrine is less far-reaching and less strict than the principle of due□

administration of justice that applies to the court. In any case, the governed always has the□

possibility to lodge an appeal with a judge that meets the requirements of Article 6.1□

ECHR.7□

35. The Court of Justice ruled that even the composition of a judicial formation does not□

should be completely amended after referral.8 According to the Court, “the fact that an□

the same judge sits in two formations [of the General Court] which□

have successively taken cognizance of the same matter, in itself, apart from any other objective□

element, do not cast doubt on the impartiality of the General Court.” “There is nothing to indicate that□

the referral of the case to a judicial formation that is in a completely different way□

composed than that which first became aware of the matter, within the framework of the□

Community law must or can be regarded as a general obligation.”□

36. In support of their assessment, the EU courts refer to the case-law of the European Court□

for Human Rights (ECtHR), which has already ruled several times that “from the□

6 Article 40 § 1 Data Protection Authority Establishment Act□

7 RvS 23 April 2009, no. 192.590, Crauwels, para. 3.2.4. See also I. OPDEBEEK and S. DE SOMER, General administrative law

and principles, Antwerp, Intersentia, 2017, 384-385.□

8 H.v.J., C-341/06 P and C-342/06 P, Chronopost and La Poste/UFEX and Others, 1 July 2008, EU:C:2008:375, §§ 51-60.□

impartiality requirement, the general principle cannot be inferred that a judicial

body that overturns an administrative or judicial decision is obliged to refer the matter to a

other body or to a body of that body composed of other persons

refer". For example, with regard to a disciplinary court, the ECtHR has ruled that the

the circumstance that three of the seven members of that college, after a previous ruling in which

they had been involved, was quashed in cassation, after referral again about the same

had to judge the case did not raise a legitimate fear of bias.9

37. Although there is no established illegality of the acts of the

Disputes Chamber or doubts about the impartiality of the Disputes Chamber, the chairman has

of the Disputes Chamber decides to comply with the request of . as much as possible

defendant and in this case two other members have been appointed - namely Mr Dirk Van Der Kelen and

Mr Yves Poullet - to sit in on the substance of the present proceedings.

The chairman will therefore continue to sit himself now that it is practical for the Disputes Chamber

it is unfeasible to sit in a completely different composition, taking into account the number of

members of both language roles.

2.2 Defenses and analysis Dispute chamber

First ground of appeal: Defendant has taken all necessary technical and organizational measures

in accordance with Articles 5 (1) (f), 24 and 32 of the GDPR and therefore an appropriate level of security

commanded.

38. Defendant first pleads all necessary technical and organizational measures

in accordance with Articles 5 (1) (f), 24 and 32 of the GDPR and therefore an appropriate

level of security. That an appropriate level of security was

According to the defendant, the offer can be demonstrated on the basis of a number of aspects.

First of all, the defendant applies internal rules regarding the technical and organizational

measures that must be complied with within the organization. Defendant takes

at all times the appropriate technical and organizational measures to protect the personal data
of its subscribers. The measures taken are evaluated every year and
adjusted if necessary. The Belgian
Institute of Postal Services and
Telecommunications (BIPT) carries out an annual audit of the technical and organizational
measures within the organisation. Due to its confidentiality, the document may
according to the defendant not be brought into these proceedings. In addition, the defendant has
duty to maintain confidentiality of communications arising from Article 124 of the Electronic Act
Communications (WEC).
9 ECtHR, Dienet v. France, September 26, 1995, § 38.
Decision on the merits 101/2022 - 12/29
39. The documents YBelgium overview of Technical and Organizational measures and Group
Security Standard10 are new documents that the Disputes Chamber is not previously aware of
could have taken. The document Group Security Standard contains the mandatory
security measures of the Y Group. It is a shared reference point of Y Group and
describes the minimum mandatory security requirements to be implemented by each entity. It
document contains general principles regarding security, information security and physical security.
The document Y Belgium overview of Technical and Organizational measures also contains
general principles.
About the verification of identity
40. The defendant stated in its statement and during the hearing that it is not possible
was to verify the identity of the third party and that of the holder of the number associated with the
to compare prepaid plans. Defendant points out, however, that the internal
procedure has been changed following the decision of 22 January 2021 of the
Dispute chamber in which, among other things, it was ordered to comply with the processing
with Articles 24 and 32 GDPR. Since then, the Defendant has therefore used as

standard procedure that identity verification is performed upon conversion

from prepaid to postpaid cards. In addition, employees in the shops have been given access to

performing that check. The reason no verification checks were performed before

according to the defendant has everything to do with the prohibitions imposed by Article 127 of

the Electronic Communications Act and the executive Royal Decree11. the executive

Decree contains further rules on the identification of the end-users of prepaid

(prepaid) cards.12 According to the defendant, the law and the decrees prescribe that

identification data may not be used for commercial purposes. Defendant

states: “Due to the strict application of the above legislation, employees

at the points of sale of the concluante when requesting the migration from a prepaid to a

postpaid subscription only check the telephone number and the SIM card number.”

41. The part of the preamble to the Royal Decree quoted by the defendant reads: “The

operators and the providers referred to in Article 126, § 1, first paragraph, may therefore

identifiers collected under Section 127 of the WEC and which are

not use for commercial purposes held under Article 126 of the WEC …….”.

10 Those documents were submitted to the proceedings by way of submission.

11 Electronic Communications Act of June 13, 2005, entered into force on June 30, 2005 and executive Royal

decision

12 Royal Decree of 27 November 2016 on end-user identification of mobile public electronic

communication services provided on a prepaid card basis, BS 7 December 2016.

The Disputes Chamber points out that the aforementioned article will, however, be continued as follows: “but they

may collect identification information from prepaid card users and

keep for commercial purposes in accordance with Article 122 (applicable

when an invoice is sent) or the general legislation on the protection of

personal living ambiance."

42. During the hearing, the defendant with regard to the abovementioned Article 127 WEC, read in
coherence with the executive Royal Decree and the Report to the King accompanying that decree,
indicated that the provision has given rise to discussion among all telecom operators,
namely whether the article should be read strictly or not. Defendant interprets it
law strictly. Since in this case it would concern the sale of subscriptions, this
considered by the defendant to be a commercial objective.
43. The defendant's assertion that carrying out an identity check (i.e. in this case the
comparing the identity data of the complainant and the third party) in the context of a conversion
from prepaid to a postpaid subscription, was not allowed to take place because of the legal
ban on use for commercial purposes, the Disputes Chamber considers incorrect.
44. Contrary to the defendant, the Disputes Chamber is of the opinion that there is no question of
a commercial purpose. First of all, the purpose of using the identity data of
a prepaid customer in this case only to prevent misuse of the telephone number by
any unauthorized persons, as in the present case. The aim is therefore to prevent the
wrongfully taking over a telephone number of a prepaid customer by a third party, resulting in
it would also have access to its mobile traffic and possibly other services linked
to the phone number. The defendant therefore had the data of the third party and the
have to compare known data of the complainant in an unambiguous way (and therefore not
based only on a SIM card number which is anything but a strong identifier.
In short, this is a legitimate purpose, namely to detect possible
fraud with telephone numbers which can have enormous consequences for those involved.
45. The Disputes Chamber hereby also refers to the Report to the King at the executive
Royal Decree.13 The report reads as follows: ”It is the intention of the legislator
not been here to impose a total ban on identity checks, but to
strict
regulations

to submit

in order to ensure a good level of protection of

to guarantee personal data." By failing to check, the defendant

disregarded the will of the legislator, which is to offer a good

level of protection of personal data to data subjects. In a case like this, the –

13 Report to the King by Royal Decree of 27 November 2016 on the identification of the end-user of mobile phones

public electronic communications services provided on the basis of a prepaid card, BS 7 December 2016.

Decision on the merits 101/2022 - 14/29

limited - processing of personal data for the purpose of verifying identity precisely to

prevent misuse of personal data.

46. In its submission, the defendant further claims:

"If, however, the Disputes Chamber is of the opinion that the concluding party was nevertheless obliged to provide the identity

with the identity of the holder of the telephone number, she interprets the

regulations and guidelines to which the controller is subject

particularly smooth. In no way does this appear to be the intention of the legislator,

as a result of which the concluding party could not be expected to hold such an opinion."

47.

Contrary to the statement of the defendant, the Disputes Chamber rules that Article 18 § 1 of

the Royal Decree implementing and explaining Article 127 § 1 of the WEC very clearly

and leaves no room for doubt as to its interpretation and application. The article

namely determines:

"The company concerned shall ascertain, through technical and operational

measures, that the person responsible for the extension or migration of the product

is actually the person identified for that product."

48. Next, the article-by-article discussion of the Royal Decree gives the following clear

explanation to this article:

”Art. 18. Product Expansion or Migration. It is possible that a person is already a customer of a

concerned company for another product (for example, a subscription to mobile

telephony) and has been identified by the company concerned for that product. That person

can then decide to purchase an additional prepaid card (product extension) or to

from the first product to a prepaid card (product migration).The

The company involved can then establish a link between the prepaid card and the product

that has already been purchased by the end user. The undertaking concerned shall ensure that

by instituting technical and operational measures, that the person carrying out the extension of

the product asks is actually the person identified for that product. This is possible

be done, for example, through the presentation of an identity document or on the basis of the

identification number and a password. The person who is the holder of the product with which

the prepaid card is associated with must be the same person as the one who

requires activation of the prepaid card. Therefore, this method should not be used if

a child requests the activation of the prepaid card and in doing so makes use of a

other product to which a parent has subscribed.”14 (own underlining)

14 Report to the King by Royal Decree of 27 November 2016 on the identification of the end user of mobile phones

public electronic communications services provided on the basis of a prepaid card, BS 7 December 2016. (Own

underlined by the Disputes Chamber)

Decision on the merits 101/2022 - 15/29

49. It is therefore clear and unequivocal from the foregoing that the undertaking concerned

(in this case the defendant) even has a legal obligation to, in the case of product migration,

to obtain certainty about the identity of the person requesting the migration.

The foregoing serves to obtain certainty as to whether it is actually the person who is responsible for that

product has been identified. It also appears from the explanatory memorandum that the verification only

can take place after submission of a

identity document or on the basis of a

identification number and a password.

50. Given the clear and unmistakable wording of the legislator in the above

regulations in which, according to the Disputes Chamber, no room is left for another

interpretation, identity verification should have taken place. The Dispute Room

considers that the defendant should have proceeded to verify the identity

of the person who requested the SIM card migration. After all, the legislator writes

expressly states that this check must be done on the basis of the identity card or

identification number and password.

51. Defendant could therefore not suffice with asking for the SIM card number and the

phone number. Indeed, the defendant had the identity card of the third party,

but has failed to compare the personal data with those of the holder of the mobile phone

number, in this case the complainant.

52. By carrying out a verification, it would soon become apparent that there are two different

persons went. Defendant failed to make such a low effort

to carry out verification, while the defendant as a telecom operator had to be aware of

the enormous consequences that such negligence could entail.

As a result, the defendant has deliberately failed to comply with a legal obligation,

namely that of Article 18 § 1 Royal Decree implementing the Telecommunications Act. The

The Disputes Chamber comes to the conclusion that there was not only an attributable

shortcoming but also a violation of Article 18 § 1 of the Royal Decree which is clearly

prescribes that a check must take place during product migration.

53. During the proceedings, the defendant has consistently argued that product migration should

be regarded as a commercial purpose and that it was therefore prohibited to

perform identity verification. However, it appears from Article 18 §1 of the Royal Decree that the legislator

does not classify product migration as a commercial purpose and rather prescribes that a

identity verification must take place. The defendant's argument therefore fails.

54. The Disputes Chamber ruled in its primary decision, among other things, that the defendant
processing in accordance with Articles 5.1.f, 5.2, 24 and 32 GDPR.
Defendant complied with this order by instituting additional proceedings
to verify the customer's identity during product migration. Defendant argues that
Decision on the merits 101/2022 - 16/29
in its conclusion, however, that this was done at the risk that the defendant could be blamed by BIPT or by a
court can be called back in connection with the use of the identification data
for commercial purposes, which would be expressly by Article 126 of the WEC
forbidden.
55. The Disputes Chamber concludes that a product migration according to the applicable legislation is not
can be regarded as a commercial purpose. It therefore reaffirms that the
Articles 5 (1) (f), 5.2, 24 and 32 of the GDPR have been infringed.
Second ground: Defendant took proactive measures in accordance with Article 5 (2) of the GDPR in order to
compliance with the regulations of the GDPR, including the technical and organizational measures
to ensure.
56. The defendant submits by its second plea that proactive measures were indeed taken
taken to ensure compliance with the requirements of the GDPR - including the technical and
organizational measures - to ensure. Defendant has, in its statement of defense,
added the Safety Working Method, among other things. This internal piece for the employees
describes how personal data of customers should be handled and reaches
handles to protect the confidentiality of the data within the defendant's organization
to ensure.
57. In Different Places
in the working method it is pointed out that a complete
identity check
(name first Name,

phone number, if there is one

is: customer number,

date of birth, identity card number, address, amount of the last invoice and where and

when the activation

has been requested) required

is for “all questions

in the

light from

contract amendment, such as; rate plan change, address change, P2P, PPP, activation

or deactivation of a service, ask for a copy of an invoice and ask for confidential

information".

58.

In the present case, the third party who (later) obtained access to the complainant's telephone number, the

conversion of his prepaid card to a postpaid subscription. He therefore asked for

activation of a new service. This means that the defendant also, according to its own

working method should have asked for additional data with the aim of establishing the

identity of the person in question. By failing to verify the identity of the third party

defendant acted culpably negligently.

59. Respondent also has the documents Y Belgium overview of Technical and

Organizational measures and Group Security Standard introduced into the procedure (see point

39 above).

Decision on the merits 101/2022 - 17/29

60.

According to the defendant, it can also be deduced from these documents that the defendant

is concerned to take appropriate technical and organizational measures at all times

to protect the personal data of its subscribers. The measures taken are

also evaluated by it every year and, if necessary, adjusted. Both documents contain

general minimum security requirements to be implemented. The Disputes Chamber can, on the basis of

these documents, however, do not come to a different conclusion than that the defendant is in default in this case

shot due to insufficient implementation of the technical and organizational measures

bring.

61. The defendant argues that the infringement had a very limited impact on the complainant. The third

According to the defendant, the person could not gain access to the complainant's profiles on

different platforms like WhatsApp and Paypal because those platforms have the two-step verification

would use in order to log in or sign up to their profiles. The third had

furthermore, according to the complainant, no access to all communications of the complainant that have been made in the past

had taken place. Therefore, according to the defendant, there is no question of

violation of the complainant's privacy. There are only practical inconveniences that the complainant

would have encountered.

62. The Disputes Chamber points out in this regard that - in contrast to the defendant's

claimed - for the use of, for example, the WhatsApp application in principle that is sufficient

someone has the phone number. The two-step verification that according to the defendant

must be completed must be activated explicitly via the WhatsApp settings and

is not enabled by default. The default security setting

so is that just it

telephone number is sufficient for taking over the use of the Whatsapp application. The

user enters the phone number through which he wants communication through the application

and then an SMS message is sent to that number. After the code

entered in the text message, communication can take place directly via

whatsapp. So, if the two-step verification has not been activated, nothing else is needed

then access the mobile phone number to which the verification code is sent.

63. Moreover, by having a telephone number, there is a significant chance that

access to different types of personal data can be obtained. Various

authorities - such as hospitals - remind of appointments by means of the

sending SMS messages. In addition, having a phone number for a

others wide open the door to fraud and fraud, for example because conversations and

messages could be conducted or sent on behalf of the injured party. The

The Disputes Chamber therefore disagrees with the defendant's assertion that there is no way

would be a violation of privacy.

64. The Court of Justice emphasized the importance of telecom data with the following

wording in its Digital Rights Ireland judgment of 8 April 2014: “From this data, in their

Decision on the merits 101/2022 - 18/29

considered as a whole, very precise conclusions can be drawn about the private life of

the persons whose data is kept, such as their daily habits, their

permanent or temporary residence, their daily or other movements, the activities that

they exercise, their social relations and the social circles in which they live.”15 Notwithstanding

the third party in the present case may not have had access to all the information referred to in the judgment, the

The Disputes Chamber believes that by having the complainant's telephone number

there was a significant risk of a violation of his privacy rights.

65. In its conclusion, the defendant argues that in principle only the user of a mobile telephone number

should know the associated SIM card number. The SIM card number will be

therefore used as verification that the applicant is indeed the actual user of the

telephone number provided. The seller would therefore have both the

phone number and have requested and obtained the SIM card number from the third party. The

migration was then carried out and the third party therefore has its own identification data

filed, according to the defendant. The third party's identifiers were

defendant checked by comparing the identity card data with the specified one

name, address and place of residence of the third party. According to the defendant, these identity details were

however, not compared to the

identity data of the prepaid customer to whom it

SIM card number and mobile number was assigned first, namely the complainant. Latter

According to the defendant, the check did not take place because identity data may not be used

used for commercial applications based on the Electronic Communications Act16 and

the Report to the King to the Royal Decree implementing this law,17 as

set out in marginal 42 et seq. above.

66. The defendant finds it incomprehensible that the third party could find out the SIM card number.

According to the defendant, the SIM card number can only be retrieved via the systems of

defendant where it is stored or if these have been communicated by the complainant himself. In order

to obtain both the telephone number and the SIM card number, the third party – according to

defendant - either had the cooperation of the complainant or that of a Y employee.

According to the defendant, the combination between SIM card and telephone number is unique, which means that the

method of using the telephone number-SIM card number combination is appropriate to

verify the user's identity. If only use were made of the

phone number to verify the user's identity before the migration, according to

can point out to the defendant inadequate technical and organizational measures. The

15 EU Court of Justice, Digital Rights Ireland and Seitlinger and Others, Joined Cases C 293/12 and C 594/12, ECLI:EU:C:20

16 Article 127 in conjunction with article 126 § 2.7° Law on electronic communications of 13 June 2005, which entered into force

June 2005.

17 Report to the King by Royal Decree of 27 November 2016 on the identification of the end-user of mobile phones

public electronic communications services provided on the basis of a prepaid card, BS 7 December 2016.

combination of telephone number and SIM card number can, according to the defendant, be

equated with the combination of e-mail address and password. Also in this combination there is

the verification consists of an element that is public and an element that only the owner can know.

67. The Disputes Chamber refers to the statement of the defendant that:

•

employees were obliged to request the SIM card number from the customer and

were required to implement a migration from prepaid to postpaid;

•

at the time there was no possibility for the employee to use the

mobile number to request the SIM card number from the database.

The question therefore remains how the third party arrived at the combination of mobile number and SIM card number.

In any event, the defendant has not been able to demonstrate this to the Disputes Chamber,

as required by Articles 5.2 and 24 GDPR.

68. Defendant

lays

a

previous notification

d.d.

11 March

2019

at

the

Data Protection Authority of a similar data breach about.18 It is mentioned

that another reason for not reporting the leak in this case was the following: “The

Data Protection Authority has not followed up this file further, which shows the

limited weight that the Data Protection Authority attaches to such

(little)

data leak. For that reason, the concludant's presumption that there was no

reporting obligation would have been confirmed in the present case.” The Disputes Chamber hereby refers to the

accountability of the defendant arising from Article 5.2 and Article 24 GDPR whereby□

it is up to the defendant to demonstrate that it also acts in accordance with Article 5.1.f GDPR□

namely: ”by taking appropriate technical or organizational measures in a□

processed in such a way as to ensure appropriate security, and that□

they are protected, among other things, against unauthorized or unlawful processing and against□

accidental loss, destruction or damage (“Integrity and Confidentiality”).” The□

assertion□

Which□

a□

previous notification□

not □

became□

treated□

by means of□

the□

Data Protection Authority, does not affect the accountability obligation.□

69. The Disputes Chamber points out once again that the accountability obligation under Articles□

5, paragraph 2, Article 24 and Article 32 GDPR entails that the controller□

takes necessary technical and organizational measures to ensure that□

the processing is in accordance with the GDPR. The foregoing obligation belongs to the□

proper fulfillment of the defendant's responsibility under Article 5(2), 24 and 32□

GDPR. The Disputes Chamber points out that the accountability obligation of article 5 paragraph 2 and article 24□

GDPR is one of the central pillars of the GDPR. This keeps□

in that on the□

18 As item 5 in its conclusions.□

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.

70. The Group 29 stated in the Opinion on the “accountability principle”

that two aspects are important in the interpretation of this principle:

(i)

“the need for a controller to provide appropriate and

effective measures

at

to take

in order to

the

principles

in front of

implement data protection; and

(ii)

the need to be able to demonstrate on request that appropriate and effective

measures have been taken. The controller must therefore

provide evidence of (i) above”.19

71. In view of the above considerations, the Disputes Chamber is of the opinion that the defendant has infringed

has committed to Articles 5.1.f, 5.2, 24 and 32 GDPR due to insufficient technical and

to take organizational measures to prevent the processing of personal data

in

in accordance with the relevant laws and regulations.

Data leak

72.

Article 33(1) of the GDPR provides: “If a personal data breach has occurred

occurred, the controller shall report it without undue delay and,

if possible, no later than 72 hours after becoming aware of it, to the corresponding

Article 55 competent supervisory authority, unless it is not probable that the infringement in

connection with personal data poses a risk to the rights and freedoms of natural persons

persons. If the notification to the supervisory authority is not made within 72 hours,

it shall be accompanied by a justification for the delay.”

73. The defendant argues in its claims that there was no obligation to report the data breach

to be given to the Data Protection Authority. The reason for this, according to the defendant, is

fact that the data breach involved one data subject, it was very short-lived and, according to

defendant did not disclose sensitive data. With regard to the foregoing, the

Disputes Chamber on the above consideration, namely that it can be considered plausible

that, for example, SMS messages are received which contain special personal data

could contain.

19 Opinion 3/2010 on the “accountability principle” adopted on 13 July 2010 by the Working Party 29, p. 10 – 14

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

74. When assessing whether an infringement poses a likely high risk to the

rights and freedoms of individuals according to Group Guidelines 29

take into account the answer to the question whether the infringement may lead to

physical, material or immaterial damage to persons whose data is the subject of

be the infringement. Examples of such damages include discrimination, identity theft, or -

fraud, financial loss and reputational damage.20 By assigning the complainant's telephone number

to a third party, the complainant is exposed to the risk of carrying out fraudulent

acts under his name, using his telephone number. Also exists –

other than defendant

seems to pose - a risk that sensitive data

(like

health data) come into the hands of third parties. Defendant argues that there is no obligation to report

existed before it, among other things because it concerns a data breach of a single

person. The Disputes Chamber points out that an infringement, however, is serious even for one person

consequences, depending entirely on the nature of the personal data and the context

in which they have been compromised. Here too it comes down to looking at the

probability and seriousness of the consequences.21 Moreover, this concerns a risk of

structural nature to which all prepaid card users may be exposed

become. It cannot be excluded that there are other cases where the Disputes Chamber

is not aware of.

75. The Disputes Chamber is of the opinion that in the present case the defendant has not succeeded in

demonstrate that sufficient proactive measures have been taken to ensure compliance with the GDPR

guarantee. The defendant's employees first of all failed to carry out a verification

between the identities of the third party and those of the complainant and Y subsequently failed to

report the data breach to the Data Protection Authority. Defendant has no

documents submitted showing that the documentation obligation imposed on the defendant has been complied with

rested. The only document submitted by Defendant regarding a data breach,

used to be

a notification

from

a

other

data leak

by means of

defendant

at

the

Data Protection Authority dating from the year 2019. From the documents of the file,

what was put forward at the hearing and the fact that the defendant did not provide documentation of the

submitted a data breach, it appears that the defendant also does not comply with the obligation of Article 33

paragraph 5 GDPR, which provides:

“The controller shall document all breaches related to

personal data, including the facts of the breach related to

personal data, the consequences thereof and the corrective measures taken. That

20 Guidelines for the reporting of personal data breaches under Regulation 2016/679, wp250rev.01,

Working group 29, p.26.

21 Ditto, p. 30

Decision on the merits 101/2022 - 22/29

documentation enables the supervisory authority to verify compliance with this article

to check."

76. The Disputes Chamber be there

already before

in decision 2020/22 on that:

"the

accountability

applied

on

data leaks

means

Which

on

a

controller with regard to these data breaches not only

is obliged to report this, if necessary, to the

supervisory authority and the data subjects, but that the latter must also at all times

be able to demonstrate that he has taken the necessary measures to be able to comply with these

obligation”22 The Disputes Chamber is of the opinion that this is not the case in the present case

demonstrated.

77.

In a non-exhaustive list that controllers can take to comply with the

accountability obligation, the Group 29 refers to, among other things, the

following measures to be taken: implementing

laying and supervising

control procedures to ensure that all measures are not only on paper but

are also implemented and functioning in practice, establishing internal

procedures, drawing up a

written and binding policy regarding

data protection, developing internal procedures for effective management

and reporting security breaches.

78. The Disputes Chamber also refers to a form attached to the Opinion in which

a similar data breach was reported, namely the telephone number of a

customer who had switched to another operator. This phone number was incorrectly referred to as

freely seen and assigned to a new customer. In the form, the defendant asked the question “What?

is the degree or level of seriousness of the data breach for data subjects at

assessing the risks to the rights and freedoms of data subjects?”

answered with “critical” data breach. According to the Disputes Chamber, this clearly shows that

the defendant also understands the seriousness of such a data breach.

79. The Disputes Chamber therefore establishes infringements of Article 33 paragraphs 1 and 5 of the GDPR. The

The Disputes Chamber points out that on behalf of the controller there is a

obligation to document any data breach, whether risky or not, in order to

to be able to provide information to the GBA. After all, the processing of personal data is

a core activity of the defendant. In addition, personal data can contain a large degree of

22 Decision 22/2020 of 8 May 2020 of the Disputes Chamber, p.12

Decision on the merits 101/2022 - 23/29

have sensitivity to those involved, partly because they have a regular and systematic

enable observation.23

80. Defendant submits a Data Breach Assessment document with its claim. In this document

documented the data breach on April 15, 2020, 7 months after the data breach

took place. The document reads, among other things:

“The incident gave a third party access to the customer's communications content from a pre-

paid card for 3.25 days. The third party had no intention of using the data,

misuse or disseminate. The data were therefore not publicly available on the

internet.

The theoretical impact of the infringement is therefore very large, as it concerns the content of the

communication, and while the likelihood that the breach will affect the

person is low, the result is an overall very high risk.

But based on the information received from the data subject, the third party

shared communication content probably limited to two-step authentication codes and this

over a period of 3.5 days. These two-step authentication codes cannot be

used by the third party who does not have access to the data subject's login data.

The consequences for the data subject are therefore limited and the risk has been adjusted to a low risk.”

81. It once again appears from the text quoted above that the defendant was indeed aware

of the fact that there was a “very high risk” in this case, as it concerned content

of telecommunications. The risk was adjusted back to "low" after the defendant became aware

found that the shared content was likely limited to two-step authentication codes.

Since third parties could not have access to the complainant's login details, it was

level adjusted. As the Disputes Chamber noted earlier, not only the

applications that require two-step authentication pose a risk to the complainant, but also

telephone and SMS traffic was exposed to great risks of, among other things, fraud that

could have been committed under his name. The Disputes Chamber rules that there is

was of high risk.

82. The Defendant is of the opinion that it had no obligation to inform the complainant of the data breach

to notify. Defendant has therefore failed to inform itself

to inform the complainant by means of a communication of the award of the

telephone number to a third party. The Disputes Chamber rules that the notification to the person concerned

23 Decision 18/2020 of 28 April 2020 of the Disputes Chamber

Decision on the merits 101/2022 - 24/29

in this specific case should be omitted in view of the special circumstance of this

case where the data subject was already aware of the data breach. The Dispute Room

therefore considers that no infringement of Article 34 GDPR has been established.

83. The Disputes Chamber refers to the example below which illustrates the importance of the notice of

a data breach to the data subjects and the competent authority.

It is an example in the recently published “Guideline on Examples regarding Data

Breach Notification” of the EDPB24 in which the contact center of a telecommunications

company gets a call from a person who claims to be a customer and requests a change of his

e-mail address so that the bills will be sent to that new e-mail address from now on

sent. The caller passes on the correct personal data of the customer, after which the invoices

will be sent to the new e-mail address from now on. When the actual customer calls the

company to ask why it is no longer receiving invoices, the company realizes that the invoices

be sent to someone else.

84. The EDPB considers the following regarding the above example:

“This case serves as an example on the importance of prior measures. The breach, from a risk aspect, presents a high level of risk, as billing data can give information about the data subject's private life (e.g.habits, contacts)and could lead to material damage (e.g. stalking, risk to physical integrity). The personal data obtained during this attack can also be used in order to facilitate account takeover in this organization or exploit further authentication measures in other organizations. Considering these risks, the “appropriate” authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication. As a result, both a notification to the SA and a communication to the data subject are needed from the controller. The prior client validation process is clearly to be refined in light of this case. The methods used for authentication were not sufficient. The malicious party was able to pretend to be the intended user by the use of publicly available information and information that they otherwise had access to. The use of this type of static knowledge-based authentication (where the answer does not change, and where the information is not “secret” such as would be the case with a password) is not recommended.”25

24 EDPB Guideline on Examples regarding Data Breach Notification, 01/2021, published at www.edpb.europa.eu.

25 EDPB Guideline on Examples regarding Data Breach Notification, 01/2021, p.30

Underlining by the Disputes Chamber

Free translation: This case serves as an example of the importance of taking preliminary measures. The infringement constitutes high risk from a risk perspective, as billing data can provide information about the private life of the data subject (e.g. habits, contacts) and can lead to material damage (e.g. stalking, risk to physical integrity). The personal data obtained in this attack may also be used to prevent account takeover in this organization or to leverage further authentication measures at other organizations. Given these risks, the 'appropriate' authentication measure meet requirements and depending on this it can be determined from which personal data can be processed.

85. Notification of breaches should be seen as a way of monitoring compliance

on the protection of personal data. Therefore, according to the

The Disputes Chamber is in no way a matter of “notification fatigue” as stated by the defendant

cited. The Group 29 states in this regard:

“Data controllers should remember that reporting a breach to the

supervisory authority is required, unless the breach is unlikely to pose a risk

to the rights and freedoms of natural persons. If it is probable that a

infringement results in a high risk to the rights and freedoms of natural persons,

natural persons must also be informed. The threshold for communicating a

infringement to persons is therefore higher than that for reporting an infringement to the

supervisory authorities, and so not all breaches need to be reported to individuals

reported, protecting them from unnecessary notification fatigue.”26

When there is a

infringement

in connection with personal data takes place or has

occurred, this may result in material or immaterial damage to natural persons or

any other economic, physical or social harm to the person concerned. Therefore

as a rule, the controller shall submit as soon as it becomes aware of a breach

connection with personal data with a risk to the rights and freedoms of data subjects,

the supervisory authority without undue delay and, if possible, within 72 hours

of the infringement. This allows the supervisory authority to fulfill its duties

and properly exercise powers, as laid down in the GDPR.

Response to fine form and right of defence

86. Defendant responded on May 31, 2022 to the intention to impose a

fine.

87.

In it, the defendant repeats that the composition of the Disputes Chamber, in his opinion, is

irregular

and the procedure as well, since the President

has remained seated

notwithstanding the decision of the Market Court. According to the defendant, it has not been proved that

As a result, both a notification to the supervisory authority and a communication to the data subject are required by the

controller. The pre-customer validation process clearly needs to be refined in light of this case. The

methods used for authentication were not sufficient. A malicious person could have impersonated the

intended user by using publicly available information and information to which they otherwise access

had. Using this type of static, knowledge-based authentication (where the answer doesn't change and where the

information is not “secret” as would be the case with a password) is not recommended.”

26 Guidelines for the reporting of personal data breaches under Regulation 2016/679, Article Working Party

29, WP25 0.rev.01

there was a data breach and the determination of the existence of a data breach is based on

purely on suspicion. No evidence has been provided by the complainant of the existence of a

data leak. The defendant is of the opinion that he has sufficient technical and organizational

took measures to prevent an incident such as the one in this case. Defendant repeatedly argues

to have complied with the rules of the Electronic Communications Act (WEC) and gives

are aware that the aforementioned law checks and verify the identity in the context of

prohibited for commercial purposes. According to the defendant, the migration of a SIM card should

be regarded as a commercial purpose. Defendant indicates that it

security policy applied to them in a previous decision of the Disputes Chamber as

was properly regarded. Defendant reiterates that there was no

obligation to report the data breach to the Data Protection Authority as it concerns 1

data subject, the data breach was short-lived and there would be no sensitive data

personal data.

88. The defendant does not agree with the finding of the Disputes Chamber that there is

been of a “disproportionate degree of negligence” as Defendant makes every effort

to protect personal data as well as possible. In addition, there was no intention

or ill will on the part of the defendant. The defendant is of the opinion that the intended fine of

EUR 20,000 disproportionate to the infringements identified. Imposing a

fine according to defendant

in stark contract with previous decisions of the

Dispute chamber in which such cases with 1 person involved and a limited

social impact would have been shelved. Defendant claims to be a victim of

a rogue person who managed to obtain the complainant's personal data.

There is also no question of any previous infringements committed by the defendant. This whole makes it

imposing a fine of EUR 20,000 is unreasonable. Defendant finds a warning

more in place. If the Disputes Chamber nevertheless wishes to impose a fine,

defendant to limit the fine to an amount of EUR 5,000. What

Concerning the annual figures, the respondent indicates that there is a slight deviation from the annual figures that

were submitted by the Disputes Chamber in the sanction form; the correct amount is

EUR 1.3XX.XXX.XXX instead of EUR 1.2XX.XXX.XXX.

89. The Disputes Chamber is of the opinion that all arguments put forward by the defendant in the

sanction form have already been dealt with in this decision and were taken into account

taken when determining the administrative fine in accordance with Article 83.2 of the GDPR.

After all, the Disputes Chamber has explained in the decision that the data breach is due

negligence on the part of the defendant. According to the Disputes Chamber, the defendant had

after all, both on the basis of the WEC and according to internal regulations, the identification data

must verify to make sure that the person standing in the store is actually

the holder of the phone number. Defendant failed to do this. In addition, it has been omitted

to report this to the Data Protection Authority. The Dispute Room

does not share the view of the defendant where it states that there is no evidence to show

that third parties have taken cognizance of the personal data as a result of which the existence of a

data breach cannot be proven. As the Disputes Chamber stated under point 63,

there was a significant chance that the third party had access to (sensitive) personal data of

complainant; after all, this third party had access to the telephone number for four days.

It cannot therefore be ruled out that access by that third party to the personal data of

complainant has taken place.

90. In this case, it concerns a controller who processes data en masse on a daily basis

who can and may be expected to have the appropriate technical and organizational

takes measures to guarantee the protection of personal data. Seen

For the foregoing, the Disputes Chamber is of the opinion that a fine of EUR 20,000 can be imposed

regarded as a very small fine in relation to the infringements found and the turnover

which is apparent from the defendant's annual figures.

91. Finally, the Disputes Chamber points out that it is not under any obligation, nor on the basis of

of the AVG or the WOG, nor on the basis of case law of the Marktenhof, to explain the reasons

of the present decision prior to the taking of the decision concerned to the

to submit contradictions of the defendants, the sanction form serves only

the possibility of opposing the proposed fine.

3. Infringements of the GDPR

92. The Disputes Chamber considers infringements of the following provisions proven by the defendant:

a. Article 5.1.f, 5.2, 24 and 32 GDPR, in view of the defendant's insufficient precautionary measures

took to prevent the data breach;

b. Article 33.1 and 33.5 GDPR, as the defendant did not report the data breach

to the GBA.

93.

The Disputes Chamber considers it appropriate to impose an administrative fine at the

amount of EUR 20,000 (Article 83, paragraph 2 GDPR; Article 100, §1, 13° WOG and Article 101 WOG).

94. Taking into account Article 83 AVG and the case law27 of the Marktenhof, the motivation

Litigation Chamber imposing an administrative fine in concrete terms:

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

a.) The seriousness of the breach: the Disputes Chamber determines that the data breach is, among other things,

due to negligence on the part of the defendant. In addition, the defendant failed to

to report the leak to the Data Protection Authority and to indicate that in this case

there is no likely high risk to the complainant's rights and obligations

as a result of which there would be no reporting obligation for the defendant. The fact that in this case it concerns

telecom data from which precise data about a person's private life can be

are derived as well as the potential risk of committing fraudulent acts in

name of that person indicate that there is a serious infringement.

b.) The duration of the infringement: the infringement lasted four days, which is a significant period of time

in light of the potential danger indicated above.

c.) The fine to be imposed is such a deterrent to prevent such infringements in the future

to prevent. In this context, the Disputes Chamber reiterates that a fine of EUR 20,000

can be regarded as a very small fine in relation to the established

infringements and the turnover that appears from the defendant's annual figures.

95. The Disputes Chamber points out that the other criteria of art. 83.2. GDPR not of nature in this case

are that they lead to an administrative fine other than that imposed by the Disputes Chamber in

within the framework of this decision.

96. 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 to

not to be taken into account for determining the amount of the fine in the present case

procedure.

97. In its response to the intention to impose a fine, the defendant objects

made at the amount of the proposed fine. From this file, according to the

However, the dispute chamber found that there was carelessness and negligence towards

protection

of the data subject's personal data

up. It

processing

after all, personal data is a core activity of the defendant, which means that it is

It is of paramount importance that the personal data is processed in accordance with the GDPR.

98. The facts, circumstances and established infringements therefore justify a fine which

meets the need to have a sufficient deterrent effect, whereby the

defendant is sanctioned sufficiently so that practices involving such infringements

would not be repeated.

Decision on the merits 101/2022 - 29/29

99. In view of the importance of transparency with regard to the decision-making of the

Litigation Chamber, this decision is published on the website of the

Data Protection Authority. It

is

however

not

required

Which

to that end

the

identifiers of the parties are disclosed directly.

FOR THESE REASONS,

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

- pursuant to Article 83 GDPR and Articles 100, 13° and 101 WOG, an administrative

to impose a fine of EUR 20,000 on the defendant for the infringements of

Articles 5.1.f, 5.2, 24, 32, 33.1 and 33.5 GDPR.

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

a period of thirty days, from the notification, to the Marktenhof, with the

Data Protection Authority as Defendant.

(Get). Hielke Hijmans

Chairman of the Disputes Chamber