Litigation Chamber

Decision on the merits 05/2021 of 22 January 2021

this decision was repealed by decision 61/2021 of 19 May 2021

File number: DOS-2019-04867

Subject: complaint for attribution of the complainant's telephone number to a third party

The Litigation Chamber of

the Data Protection Authority, made up of

Mr Hielke Hijmans, chairman, and Messrs Jelle Stassijns and Frank De Smet, 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 the

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

data protection, hereinafter the "GDPR");

Having regard to the law of 3 December 2017 establishing the Data Protection Authority, hereinafter the

"LCA";

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

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

Considering the documents in the file;

made the following decision regarding:

-

the plaintiff: Mr. X

-

the defendant: Y

.

.

.

.□

.□

.□

Decision on the merits 05/2021 - 2/21□

1. Facts and procedure□

1. On September 20, 2019, the complainant filed a complaint with the Data Protection Authority□

against Y. The complaint was declared admissible by the Frontline Department on□

September 30, 2019. The complaint concerns the alleged attribution of the mobile number□

of the complainant by his supplier Y to a third party, with the effect that the complainant could no longer□

have his number. The plaintiff's SIM card was deactivated and the third party could therefore have□

knowledge of traffic and calls made by the complainant on his personal mobile phone, as well as□

associated accounts (such as Paypal, WhatsApp and Facebook) from September 16 to 19, 2019 inclusive.□

2. Since the complaint is against Y, whose principal place of business is in Member State Z,□

the Data Protection Authority has contacted the controller of this Member State in order to□

check whether or not the complaint should be considered cross-border. This communication□

led to an examination of the complaint and the processing of data according to the national procedure of□

the Belgian Data Protection Authority (Art. 56.2 GDPR)1, with Y as defendant.□

3. On April 15, 2020, the Litigation Chamber decided that the complaint could be examined on the□

merits and informed the complainant and the respondent of this decision without delay by registered letter.□

Likewise, the parties were informed of the provisions of article 98 of the LCA as well as of the□

deadlines for submitting their conclusions. The deadline for receipt of the conclusions in□

respondent's response was set for May 27, 2020, that for the submissions in reply of the□

plaintiff on June 17, 2020 and that for the defendant's reply submissions on July 8, 2020.□

4. By letter dated April 20, 2020, Counsel for the Respondent identified themselves in the file,□

requested a copy of the file and expressed their wish to be heard during a hearing on□

the basis of article 98, 2° of the LCA.□

5. On May 27, 2020, the Respondent filed submissions in response.

6. Neither the Complainant nor the Respondent made use of the opportunity to make submissions in

replica. The complainant did not wish to have recourse to the possibility of being heard.

7. On November 9, 2020, the defendant was heard by the Litigation Chamber, in accordance with

Article 53 of the internal rules.

1 Article 56.2 provides the following: By way of derogation from paragraph 1, each supervisory authority is competent to process

a claim lodged with it or a possible breach of these regulations, if its subject matter concerns only

an establishment in the Member State to which it belongs or substantially affects data subjects in that Member State

uniquely.

8. On November 19, 2020, the minutes of the hearing are submitted to the parties. The parties have

not reacted.

9. On December 7, 2020, the intention to impose a fine is communicated to the defendant.

On December 22, 2020, the defendant reacted to this intention in detail.

2. Legal basis

Article 5.1.f) GDPR

1. Personal data are:

f) processed in a way that ensures appropriate security of personal data, including

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

of accidental origin, using appropriate technical or organizational measures (integrity and

confidentiality).

Article 5.2 GDPR

The controller is responsible for compliance with paragraph 1 and is able to

demonstrate that it is respected (responsibility).

GDPR Article 24

1. Taking into account the nature, scope, context and purposes of the processing as well as the

risks, of varying likelihood and severity, to the rights and freedoms of individuals

physical, the controller implements technical and organizational measures

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

in accordance with this regulation. These measures are reviewed and updated if necessary.

2. Where proportionate in relation to the processing activities, the measures referred to in

paragraph 1 include the implementation of appropriate policies for the protection of

given by the controller.

Decision on the merits 05/2021 - 4/21

3. The application of an approved code of conduct as provided for in article 40 or mechanisms for

certification approved as provided for in article 42 can be used as an element to demonstrate compliance

obligations incumbent on the controller.

GDPR Article 32

1. Considering the state of knowledge, the costs of implementation and the nature, scope,

the context and purposes of the processing as well as the risks, including the degree of probability and

gravity varies, for the rights and freedoms of natural persons, the controller and the

subcontractor implement the appropriate technical and organizational measures in order to

guarantee a level of security appropriate to the risk, including, among other things, as required:

a) pseudonymization and encryption of personal data;

b) means to ensure confidentiality, integrity, availability and resilience

constants of processing systems and services

c) the means to restore the availability of personal data and access to

these within appropriate timeframes in the event of a physical or technical incident d) a procedure aimed at

to regularly test, analyze and evaluate the effectiveness of technical and organizational measures

to ensure the safety of the treatment.

2. When assessing the appropriate level of security, particular account shall be taken of the

risks presented by the processing, resulting in particular from the destruction, loss, alteration,

the unauthorized disclosure of personal data transmitted, stored or processed

otherwise, or unauthorized access to such data, accidentally or unlawfully.

3. The application of an approved code of conduct as provided for in Article 40 or a mechanism for

certification approved as provided for in article 42 can be used as evidence of compliance with the

requirements provided for in paragraph 1 of this article.

4. The controller and processor must take steps to ensure that

any natural person acting under the authority of the controller or under that of the sub-

processor, who has access to personal data, does not process them, except on instructions from the

controller, unless required to do so by Union law or the law of a State

member."

Article 33 GDPR

1. In the event of a personal data breach, the controller shall notify the

violation in question to the competent supervisory authority in accordance with Article 55, in the

Decision on the merits 05/2021 - 5/21

as soon as possible and, if possible, 72 hours at the latest after becoming aware of it, unless

the violation in question is not likely to create a risk for the rights and freedoms of

physical persons. When the notification to the supervisory authority does not take place within 72 hours,

it is accompanied by the reasons for the delay.

2. The processor shall notify the controller of any data breach

staff as soon as possible after becoming aware of it.

3. The notification referred to in paragraph 1 must, at the very least:

a) describe the nature of the personal data breach including, if possible, the

categories and the approximate number of persons affected by the breach and the categories and

the approximate number of personal data records concerned;

b) the name and contact details of the data protection officer or other contact point

from whom further information may be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or that the controller proposes to take to remedy

the breach of personal data, including, where applicable, measures to

mitigate any negative consequences.

4. If and to the extent that it is not possible to provide all information at the same time,

information may be released in a staggered manner without further undue delay.

5. The data controller shall document any personal data breach, in

stating the facts about the personal data breach, its effects and the measures

taken to remedy it. The documentation thus compiled enables the supervisory authority to verify

compliance with this article."

Article 34.1 GDPR

34.1. When a personal data breach is likely to create a risk

high for the rights and freedoms of a natural person, the controller communicates

the breach of personal data to the data subject as soon as possible.

Decision on the merits 05/2021 - 6/21

3. Motivation

3.1 Conclusions and analysis of the Litigation Chamber

Procedure followed

10. The defendant reacted to the intention to impose a fine. The reaction implies in particular that the

defendant considers that the rights of the defense have been violated by the Litigation Chamber.

According to the Respondent, the violations found by the Litigation Chamber are few, if any

related to the complaint initially lodged by the complainant. The respondent asserts that in its complaint,

the complainant only stated that it was a question of a violation of his privacy, without specifying

what violations it was. The defendant considers that the task of the Litigation Chamber

was to qualify this complaint legally and immediately notify the defendant.

The Respondent claims to have been informed of the specific violations for the first time on

December 7, 2020, therefore through the communicated intention to impose a fine, and that he did not
therefore unable to defend himself effectively against the charges. Furthermore, the defendant believed
that it was necessary in this case for the Litigation Chamber to seize the Inspection Service.
This did not take place and after the closing of the debates, the Litigation Chamber itself qualified
legally the facts, according to the defendant.

11. The Litigation Chamber would like to draw general attention to the fact that for
data subjects whose personal data are processed, the introduction of a
Complaint doesn't have to be complicated. The complaints procedure as provided for in Article 77 of the
GDPR and as developed in the LCA is intended as an alternative to resorting to
civil or administrative courts. The right to complain to the DPA must remain easy and
accessible to the citizen. Thus, for example, the legislator did not want the parties to be
always assisted by a lawyer.2

Article 60 of the ACL sets low requirements for the admissibility of a complaint. So that a
complaint is declared admissible, it is only required that it be written in one of the languages
national, that it contains a statement of the facts as well as the indications necessary to
identify the processing to which it relates and that it falls within the competence of the DPA. The article
does not require the complaint to involve an alleged violation of a statutory provision.

12. When assessing the merits of the complaint, the Litigation Chamber will therefore only check
not whether in the complaint lodged formally with the DPA, the complainants have invoked the
good legal disposition to support their request, but if the facts in question constitute

2 See e.g. the 2021 ODA Management Plan, p. 18.

a breach of one of the legal provisions, compliance with which is subject to control by the DPA.
The Litigation Chamber further emphasizes in this respect that the control of compliance with the GDPR is the
main mission of this supervisory body.

13. In an earlier decision, the Litigation Chamber considered the following:

“Similarly, plaintiffs are not required to plead all relevant facts regarding
the violation alleged in their complaint. The Litigation Chamber must be able to help them by asking
questions directed so as to fully understand in fact and in law the potential harm to a
fundamental right that the complainant wishes to bring to his attention. The Litigation Chamber can
also take account of grievances subsequently developed by way of conclusion by the
plaintiff insofar as these are facts or legal arguments related to the alleged infringement of which
it was seized by way of complaint, and in respect of the rights of the defence.
"During the procedure following the complaint, the Litigation Chamber therefore has the possibility of
change the legal qualification of the facts submitted to it, or examine new facts
related to the complaint, without necessarily calling on the intervention of the Inspection Service,
including by asking questions of the parties or taking into account new facts or
qualifications invoked by way of conclusion, and this, within the limits of the contradictory debate,
know, provided that the parties have had the opportunity to discuss these facts or qualifications
legal in a manner consistent with the rights of defence. If necessary, it is up to the Chamber
litigation to stimulate this debate either in its letter of invitation to conclude on the basis of Article 98
of the LCA, or later in the context of a reopening of the proceedings. In this context, the
taking into account a new legal qualification invoked by the plaintiff does not harm the
procedural fairness and equality of arms, a fortiori insofar as the
decisions of the Litigation Chamber are subject to appeal with full jurisdiction to
the Court of Markets3.”
14. The Litigation Chamber considers - unlike the defendant - that in this case, the defendant has
been able to defend himself fully and against all the violations complained of and that there was no question
new facts notified subsequently against which the defendant was unable to defend himself.
By means of the pleadings in response submitted on May 27, 2020, the defendant has indeed
amply discussed all (possible) violations and defended himself against the complaint and the
charges. In his submissions - in summary - the Respondent indeed claimed to have taken all

the necessary technical and organizational measures as well as other security measures

precaution to avoid a breach of privacy. The defendant therefore considers that he acted

3 Decision 17/2020 of the Litigation Chamber https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-

fond-n-17-2020.pdf

Decision on the merits 05/2021 - 8/21

in accordance with articles 5.1.f, 5.2, 24, 32, 33 and 34 of the GDPR. In addition, the defendant has

acknowledged that there was talk of a data leak. However, he disputed that it was a

data leak likely to create a high risk to personal data

and of which notification should have been made to the Data Protection Authority (Article 33

GDPR). The Respondent cites another reason for not making a notification: in a

previous similar case of data leak where the notification had indeed been made, the Authority

Data Protection Authority had taken no further action against the Respondent.4

Contents of the case

15. The plaintiff has been a client of the defendant since June 11, 2015 and uses telephony services

mobile (prepaid). The complainant's telephone number was assigned for a period of four

days, namely from 15 to 19 September 2019 inclusive, to a third party and on this occasion, the SIM card of the

complainant has been deactivated.

16. During this procedure, the Litigation Division endeavored to understand the

sequence of events leading to the assignment of the complainant's telephone number to

a third. It is clear from this decision that the ins and outs of the

concrete course of events cannot be fully clarified. According to the

defendant, the third party went on September 11, 2019 to one of the defendant's stores in order to

convert the plaintiff's prepaid subscription to a postpaid subscription (including a

smartphone paid after 24 months of subscription). The Respondent indicates that on this occasion, both

the complainant's telephone number and SIM card number were given by the third party.

From 11 September, the plaintiff's subscription was therefore changed from prepaid to postpaid.

The third party admittedly communicated its own identity data, following which these were
associated with the postpaid subscription, so that all costs from that point onwards have been
invoiced on behalf of the third party. On September 11, however, the third party did not yet have a card
SIM linked to the complainant's mobile phone number with the effect that the complainant could still
continue to benefit from the services of the subscription. According to the defendant, four days later,
on September 15, the third party again went to a Y store and asked for a new
SIM card linked to the same mobile phone number. At that time, he therefore obtained access to the number of
Complainant's mobile phone and the latter's SIM card were terminated. From then on, the
complainant no longer had a connection to the network.

17. In his complaint, the plaintiff explains that he had several telephone contacts with the defendant
and having gone to the defendant's stores in order to be able to have his number again
4 On this subject, see point [37] below.

phone. It was not until September 19 that the complainant was able to use his
phone number.

18. During the hearing, at the request of the Litigation Chamber, the defendant gave
explanations of the standard procedure that is followed in cases comparable to this one.
The Respondent asserts - as already stated earlier in the pleadings - that in principle
only the user of a mobile phone number should be able to know the card number
SIM linked to it. This is the reason why the SIM card number is used to verify that
the caller is the real user of the phone number that is given. The seller would have
therefore had to ask the third party in store and receive from him both the telephone number
and the SIM card number. According to the defendant, the migration was then carried out and the third party
therefore given on this occasion his own identity data. According to the defendant, the data
of the third party's identification have been checked by comparing the data on the identity card with
the name, address and residence of the third party. According to the defendant, these identity data did not

however, not been compared with the identity data of the prepaid customer to whom the telephone number

SIM card and mobile phone number were assigned first, namely the complainant. According to

defendant, this check did not take place because under the Communications Act

electronics5 and the report to the King on the royal decree implementing this law, the use of

identity data for commercial applications is not permitted.6

19. The defendant considers it incomprehensible that the third party could find the SIM card number.

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

defendant where it is registered or if it is communicated by the plaintiff himself.

To obtain the telephone number as well as the SIM card number, the third party should have - according to

the defendant - benefit from the cooperation of the complainant or that of an employee Y.

20. During the hearing, the defendant stated that the introduction of a SIM card number by the

employee of a store Y is a mandatory field ("mandatory") to perform a migration

from prepaid to postpaid. According to the defendant, the employee must therefore request the data

for this field to the customer and actually complete it in order to be able to conclude the contract for

postpaid subscription. According to the defendant, an employee of store Y cannot

no longer make requests to prepaid card databases in order to obtain the

SIM card number using the GSM number. According to the defendant, the collaborator could not

5 Article 127 juncto article 126, § 2, 7° of the law on electronic communications of 13 June 2005, entry into force

June 30, 2005.

6Report to the King on the Royal Decree of 27 November 2016 relating to the identification of the end user of communications s

mobile public electronic devices provided on the basis of a prepaid card, MB of December 7, 2016.

having obtained the number of the SIM card - if the third party had not given it himself - that in

phoning other Y co-workers to ask. For the defendant, the probability that a

collaborator has helped the third party is however weak, in particular because the collaborator would not have

got no commission. Furthermore, the Respondent asserts that in the days and hours

close to the migration request, the complainant's data were not subject to any

consultation.

21. Based on the defendant's statement that store employees must

you must ask for the SIM card number to migrate from prepaid to

postpaid and there is no possibility for the employee to consult the card number

SIM in the database from the GSM number, the question remains how

the third party was able to obtain the combination of mobile phone number and SIM card number.

22. To the question posed by the Litigation Chamber during the hearing as to whether it could have been a

data confidentiality problem at Y level or in its systems - for example via a

unauthorized access to the online customer portal, which made it possible to obtain the SIM card number

- the defendant replied in the negative. According to the defendant, no SIM card number is

mentioned on the Y customer portal (both via the Internet browser and via the mobile application).

The defendant further makes it known during the hearing that he has not received any notification from other customers

regarding possible cases of unauthorized access to their SIM card number.

23. According to the defendant, another scenario is that the third party committed fraud with intent

maliciously by somehow obtaining the combination of the telephone number

and the plaintiff's SIM card number. The Litigation Division notes, however, that the

third party correctly filled in their own name, address and residence, so that from September 11,

all the invoices ended up at his house (and between September 11 and 15, the plaintiff even

principle could use the services of Y at the expense of the third party). This makes fraud on the part of the third party

less plausible. During the hearing, the defendant argues that the third party certainly communicated its

own personal data to the defendant, but this does not prevent him from being able to

always be a case of fraud. According to the defendant, the third party indeed received a

mobile phone when concluding the postpaid subscription. The principle in this respect is

that after paying the subscription fee for two years, the device would be fully

refunded. According to the defendant, the third party never paid the invoices charged for

postpaid subscription. The defendant states that he has initiated proceedings against the third party for

non-payment of bills. However, the Litigation Chamber does not understand, in this

scenario, why it was necessary for the third party to take over the complainant's telephone number.

In this case, the smartphone could also be obtained simply by requesting a subscription

postpaid with a new mobile number.

Decision on the merits 05/2021 - 11/21

24. The Litigation Chamber considers this hypothesis of fraud in order to obtain a smartphone

by the resumption of the complainant's mobile number as being in this case rather improbable,

especially since the third party has communicated its own personal data and has concluded

a contract for the mobile subscription, with the effect that from September 11, the costs

were also billed.

25. The Respondent indicated both in its pleadings and during the hearing that it was not possible

to compare the identity of the third party and that of the holder of the number linked to the prepaid subscription. For the

justify, the defendant refers to the prohibitions imposed by article 127 of the law relating to

electronic communications and the royal decree that executes it7. The implementing decree contains

procedures relating to the identification of end users of prepaid cards8. According to

the defendant, the law and the decrees prescribe that the identification data cannot be

used for commercial purposes. The defendant indicates in particular that: "Due to

the strict application of the above legislation, in the event of a subscription migration request

prepaid to a postpaid subscription, the employees of the defendant's points of sale

can only verify phone number and SIM card number.”.

26. The part of the preamble to the Royal Decree quoted by the Respondent is worded as follows:

"Consequently, the operators and suppliers referred to in Article 126, § 1, first paragraph, may not

not use for commercial purposes the identification data collected under article 127 of the

LCE, which are kept under article 126 of the LCE ...". The Litigation Chamber makes

note that the article in question continues, however, as follows: "but they may collect

and commercially store prepaid card user identification data

in accordance with Article 122 (applicable if an invoice is sent) or the general legislation on

protection of privacy."

27. During the hearing, the defendant, questioned on the aforementioned article 127 of the LCE, read jointly

with the royal decree of execution and the report to the King of this decree, declared that the provision has

sparked discussions among all the telecom operators, in particular concerning the question of

whether the article should be read strictly or not. The defendant interprets the article of law

strict sense. Since the present case involves the sale of subscriptions, the defendant considers this

as a commercial purpose.

28. For the Litigation Chamber, the position of the defendant according to which the realization of a control

of identity (therefore in this case the comparison of the complainant's identity data with those of the

7 Law relating to electronic communications of June 13, 2005, entered into force on June 30, 2005 and royal decree of executio

8Royal Decree of 27 November 2016 relating to the identification of the end user of electronic communications services

mobile public services provided on the basis of a prepaid card, MB of December 7, 2016.

third parties) as part of the transition from a prepaid subscription to a postpaid subscription could not

not take place due to the legal prohibition of commercial use is not correct.

29. The Litigation Chamber wonders whether it is indeed a question here of a purpose

commercial, since the use of the identity data of a prepaid customer would in this case

only intended to prevent abuse by a person who may be misrepresenting himself

in store Y as the user of the telephone number, linked to a prepaid card.

The purpose is therefore to prevent the undue takeover of a telephone number of a prepaid customer by

a third party, which would allow the latter to also obtain access to the customer's GSM communications

and perhaps also to other services linked to the telephone number (see below) with therefore a

access to their personal data. The defendant should therefore have compared in such a way

unequivocal (and therefore not solely on the basis of a SIM card number which is anything but a

strong authentication) the data of the third party with the data of the complainant of which he was aware.

This is indeed a legitimate purpose, namely the detection of potential fraud with

phone numbers that can have enormous consequences for the people concerned.

30. In this regard, the Litigation Chamber also draws attention to the report to the King of the decree

royal execution9. From this report, the following can be deduced: The aim of the legislator in this regard

was not to impose a general ban on identity checks but to subject it to a

strict regulations in order to be able to guarantee a good level of data protection at

personal character. The Litigation Chamber considers that by not carrying out any checks, the

defendant ignored the will of the legislator, namely to offer a good level of protection to

personal data to data subjects. In a case such as this, the

processing - limited - of personal data with a view to verifying the identity

specifically to prevent the misuse of personal data.

31. The Litigation Chamber considers that in this case, the defendant could simply have checked whether

the data on the identity card of the third party (after verification of the photo on the identity card)

corresponded to the data known to the holder of the telephone number of the prepaid card.

The defendant had the third party's identity card available but failed to compare the

personal data with those of the holder of the mobile phone number, in this case the

complainant. A check would have quickly shown that they were two people

different. The defendant neglected to carry out this non-binding verification, whereas in

as a telecom operator, the defendant should precisely have been aware of the

enormous consequences that such negligence could entail. The Litigation Chamber

considers this negligence to be disproportionate.

9 Report to the King on the Royal Decree of 27 November 2016 relating to the identification of the end user of communications s

mobile public electronic devices provided on the basis of a prepaid card, MB of December 7, 2016.

32. The Respondent attached to its submissions in response a document entitled "Method of work

Security". This internal document intended for employees defines the way in which the data
personal data of customers should be handled and provides guidance on how to ensure the
confidentiality of data within the respondent's organization.

33. Various places in this working method state that full identity verification
(surname, first name, telephone number, if there is one, customer number, address, amount of the
last invoice as well as where and when activation is requested) is required
for "Any request relating to a modification of the contract, such as: change of plan
rate, change of address, P2P, PPP, activation or deactivation of a service, request for
copy of invoice and request for confidential information" [free translation made by the service
of translation of the APD in the absence of an official translation].

34. In this case, the third party who (subsequently) had the complainant's telephone number
requested the conversion of his prepaid card into a postpaid subscription. He therefore asked
the activation of a new service. This means that, according to its own working method, the
defendant should have requested additional information in order to establish the identity of
the person in question. The Litigation Chamber considers that by failing to establish the identity
third party with certainty, the defendant was culpably negligent.

35. The Respondent asserts that the violation had very limited consequences for the Complainant.
According to the defendant, the third party was unable to access the complainant's profiles on different platforms
such as WhatsApp and Paypal as these platforms use two-step verification in order to
to be able to connect to their profiles. According to the defendant, the third party also did not have access to
all past communications from the complainant. According to the defendant, it is therefore in no way
matter of violation of the complainant's privacy. It's all about the downsides
practices that the complainant allegedly suffered.

36. The Litigation Chamber notes in this respect that - contrary to what the defendant asserted -
to use the WhatsApp application, for example, it is sufficient in principle that someone has the
phone number. The two-step verification that should be followed, according to the respondent,

must be explicitly enabled through WhatsApp settings and is not configured by default.

The default security setting is therefore that only the telephone number is sufficient to

resume using the WhatsApp application. The user enters the telephone number via

which he wants to use the communication via the app, and an SMS is then sent to this

number. After entering the code included in the SMS, it is directly possible to

Decision on the merits 05/2021 - 14/21

communicate via WhatsApp. If two-step verification has not been enabled, access to the

mobile phone number to which the verification code was sent is sufficient.

37. By having a telephone number, there is also a considerable risk of being able to

access different kinds of personal data. Various instances - such as by

example of hospitals - send appointment reminders by sending SMS. Furthermore, the fact

having a phone number opens the door wide to fraud and scams

(for example because it is possible to conduct conversations or send messages to the

name of injured party). The Litigation Chamber therefore does not agree with the assertion of the

defendant that there is no question of breach of privacy.

38. The Court of Justice underlined the importance of telecommunications data in its judgment

"Digital Rights Ireland" of April 8, 2014 in these terms: "These data, taken as a whole,

are likely to allow very precise conclusions to be drawn concerning the privacy of

people whose data has been stored, such as daily life habits,

permanent or temporary places of residence, daily or other trips, activities

exercised, the social relations of these persons and the social circles frequented by them."10.

Although in this case, the third party probably could not have had all the data cited

in the judgment, the Litigation Division considers that, having had the telephone number

of the complainant, there is a significant risk of violation of the latter's rights in

respect for privacy.

39. Article 33, paragraph 1 of the GDPR provides the following: "In the event of a data breach at

personal nature, the controller shall notify the violation in question to the authority of

competent control in accordance with Article 55, as soon as possible and, if possible,

72 hours at the latest after becoming aware of it, unless the violation in question

is not likely to create a risk for the rights and freedoms of natural persons.

When the notification to the supervisory authority does not take place within 72 hours, it is accompanied

of the reasons for the delay."

40. The Respondent states in its pleadings that there was no obligation to notify the leak of

data to the Data Protection Authority. The reason is according to him that the data leak

affected only one person concerned, that it was of very short duration and that he considered

that it did not involve sensitive data. In view of the foregoing, the Chamber

Contentitieuse draws attention to the point mentioned above, namely that one can consider

10 EU Court of Justice, Digital Rights Ireland and Seitlinger and Others, joined cases C 293/12 and C 594/12, ECLI:EU:C:201

pt. 27.

plausible that, for example, text messages containing particular personal data have been

received.

41. To assess whether a violation is likely to pose a high risk to the rights and freedoms

natural persons, according to the Group Guidelines 29 account should be taken of the

answer to the question of whether the violation may result in physical damage, material damage

or immaterial for the persons whose data is the subject of the breach. examples of

such damages are discrimination, theft or impersonation, financial loss and

damage to reputation. Assigning the complainant's telephone number to a third party exposes

the complainant at the risk of fraudulent acts being carried out in his name, using his

phone number. There is also a risk - contrary to what the

defendant - that sensitive data (such as health data) fall into the hands

of third parties. The respondent asserts that there was no notification obligation on its part,

not least because it was a single person data breach. Bedroom

Litigation points out that a violation, even if it affects only one person, can

however have serious consequences, depending on the nature of the personal data

personnel and the context in which they were compromised. Here again, it is worth considering

the likelihood and severity of the consequences12. According to the Litigation Chamber, it is also

here of a risk of a structural nature to which all users of prepaid cards can

potentially be exposed. It cannot be ruled out that there are other cases of which the Chamber

Litigation is not aware.

42. The respondent submits to the Data Protection Authority an earlier notification dated

March 11, 2019 regarding a similar data leak13. He indicates there that another reason for not

not notify the leak in this case was as follows: "The Data Protection Authority has not

followed up on this case, which shows the limited importance that the Data Protection Authority

data grants to these (small) data leaks. This confirmed the defendant's presumption

that there was no notice requirement in the present case."

carried out by the translation service of the Data Protection Authority, in the absence of

official translation]. The Litigation Chamber draws attention in this respect to the responsibility

of the defendant which derives from Article 5.2 and Article 24 of the GDPR, under which he

responsibility to demonstrate that it also complies with Article 5.1.f) of the GDPR, namely: "to guarantee a

appropriate security of the personal data processed, including protection against

unauthorized or unlawful processing and against the original loss, destruction or damage

accidental ("integrity and confidentiality"), using technical or organizational measures."

11 Guidelines for notifying a personal data breach under the Regulation

2016/679, Group 29, p. 26.

12 Same, p. 30.

13 As Exhibit 5 in his pleadings.

The assertion that a previous notification has not been processed by the Authority of

Data protection does not remove liability.

43. The Litigation Chamber recalls once again that under Article 5, paragraph 2, of

Article 24 and Article 32 of the GDPR, liability implies that the controller

take the necessary technical and organizational measures to ensure that the

processing complies with the GDPR. The aforementioned obligation is part of the proper execution of the

liability of the defendant, in accordance with Article 5, paragraph 2, Article 24 and Article

32 GDPR. The Litigation Chamber emphasizes that the liability referred to in Article 5,

paragraph 2 and Article 24 is one of the central pillars of the GDPR. This implies that the

controller has the responsibility, on the one hand, to take proactive measures in order to

to guarantee compliance with the requirements of the GDPR and on the other hand, to be able to prove that he has taken

such measures.

44. In its Opinion on the "principle of responsibility", Group 29 informs that two aspects are

important for the interpretation of this principle:

(i)

“"the need for the data controller to take steps

appropriate and effective to implement the principles of data protection

data; and

(ii)

the need to demonstrate, upon request, that appropriate and effective measures

were taken. Accordingly, the manager should provide evidence of

the execution of point (i) above"14.

45. The Litigation Chamber considers that in the present case, the defendant has failed to demonstrate

that proactive measures have been taken to ensure compliance with the GDPR. The collaborators

of the defendant first failed to carry out a check between the identity of the third party and that of the

complainant and Y subsequently neglected to notify the Data Protection Authority of the data breach.

data. The Respondent has provided no evidence that the documentation obligation imposed on it

was incumbent was respected. The only document provided by the defendant concerning a leak of

data was a notification of another data breach by the defendant to the Authority of

data protection dating from 2019. It appears from the documents in the file, from what was said to

the hearing and the defendant's failure to introduce any documentation relating to the leak

of data that the defendant also fails to comply with the obligation of Article 33(5)

of the GDPR, which provides that:

14 Opinion 3/2010 on the principle of responsibility adopted on 13 July 2010 by the Group 29, p. 10-14,

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

"The data controller shall document any personal data breach,

stating the facts about the personal data breach, its effects

and the measures taken to remedy them. The documentation thus compiled allows the authority

control to verify compliance with this article."

46. The Litigation Chamber has already pointed out previously in its decision 2020/22 that:

"Liability applied to data leaks implies that a data controller has

not only the responsibility to notify data leaks if necessary to the authority of

control and data subjects, in accordance with Articles 33 and 34 of the GDPR, but also

that he must be able to demonstrate at any time that he has taken the necessary measures in order to be able to

comply with this obligation"15. The Litigation Chamber considers that in the present case, this

cannot be demonstrated.

47. In a non-exhaustive list of measures that controllers can take

to satisfy the liability, Group 29 refers, inter alia, to the following measures to

take: the implementation and monitoring of control procedures to ensure that all

the measures do not only exist on paper but are also executed and work

in practice, the establishment of internal procedures, the development of a written policy and

binding in terms of data protection, the development of internal procedures

for effective management and notification of security breaches.

48. The Litigation Division also draws attention to a form attached to the conclusions which

mentioned a similar data leak, namely the phone number of a customer who had

changed operator. This telephone number had been wrongly considered free and assigned to

another customer. In the form, to the question "What is the degree or level of seriousness of the

data leakage for data subjects when analyzing risks to rights and

freedoms of the persons concerned?", it should be noted that the defendant replied that the leak of

data was "critical". According to the Litigation Chamber, this clearly shows that the defendant

also understands the seriousness of such a data leak.

49. The Litigation Division therefore finds a violation of Article 33, paragraphs 1 and 5, and

of Article 34, paragraphs 1 and 2 of the GDPR. The Litigation Chamber emphasizes that there is in

the head of the controller an obligation to document each data leak,

whether it involves risks or not, in order to be able to provide information to the DPA. The treatment

of personal data is indeed a central activity of the defendant. The data to

personal character may also present a high degree of sensitivity for people

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

concerned, in particular because they allow regular and systematic observation16.

The complainant should also have been informed of the data leak under section 34.1. Although

the complainant was already aware of the data breach by calling his own number, the

defendant should also have communicated this leak to him without delay, in accordance with the

requirements of Article 34, paragraph 2. The aforementioned article indeed provides that the notification must

include the nature of the breach, the contact details of the data protection officer or

another point of contact where additional information can be

obtained and the measures that the controller has proposed or taken.

50. The Litigation Chamber reasonably infers from the defendant's omission to introduce into the
procedure a communication within the meaning of Article 34 of the GDPR that such communication has not
was made to the complainant. The defendant therefore neglected, after he himself was aware,
to inform the complainant by means of a communication in accordance with Article 34(2) of
the attribution of the telephone number of the latter to a third party. The Litigation Chamber rejects
Respondent's assertion that a communication to the data subject was not
necessary in this case on the grounds that there was no question of a high risk. Bedroom
Litigation refers in this context to the following example in the "Guidelines on Examples
regarding Data Breach Notification" recently published by the EDPB, in which the center of
contact from a telecommunications company receives a call from a person claiming to be a
customer and asks to change his e-mail address so that invoices are now sent
to this new email address. The caller provides the correct personal data of the customer,
after which the invoices are sent to the new email address. When the real
customer calls the company to ask why he no longer receives invoices, the company goes
account that invoices are sent to someone else.
51. With respect to the example above, the EDPB envisages the following:
“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.
16 Decision 18/2020 of April 28, 2020 of the Litigation Chamber.

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.”17

52. Notification of breaches should be seen as a way to improve compliance with

personal data protection rules. When a relative violation

to personal data occurs or has occurred, it may cause

material or immaterial damage to natural persons or any other damage

economic, physical or social for the data subject. Therefore, as soon as the

controller becomes aware of a personal data breach

presenting a risk to the rights and freedoms of data subjects, it must, without delay

unjustified and, if possible, within 72 hours, notify the violation to the supervisory authority. This allows

the supervisory authority to correctly exercise its missions and powers as defined

in the GDPR.

4. GDPR Violations

53. The Litigation Chamber considers that the violations of the following provisions by the Respondent

are proven:

at. articles 5.1.f, 5.2, 24 and 32 of the GDPR, since the defendant did not take sufficient

precautionary measures to prevent data leakage;

b.

Articles 33.1, 33.5 and 34.1 of the GDPR, since the defendant did not notify the leak

of data to the DPA and the data subject.

54. The Litigation Chamber deems it appropriate to impose an administrative fine in the amount of

25,000 euros (article 83, second paragraph of the GDPR; article 100, § 1, 13° of the LCA and

section 101 of the LCA).

55. Taking into account Article 83 of the GDPR and the18 case law of the Court of Markets, the Bench

Litigation motivates the imposition of an administrative sanction in a concrete way:

17 EDPB Guideline on Examples regarding Data Breach Notification, 01/2021, p. 30 Emphasis by the Litigation Chamber.

18 Court of Appeal of Brussels (Cour des Marchés section), X c. DPA, Judgment 2020/1471 of February 19, 2020.

a) The seriousness of the violation: the Litigation Division finds that the data leak is

in particular due to negligence on the part of the defendant. The defendant further failed to

notify the leak to the Data Protection Authority, both in its conclusions and when

of the hearing, he affirmed that since there was no question in this case of an operation

likely to create a high risk for the rights and duties of the complainant, there would be no

no notification obligation on its part. Since this is a leak of

telecommunications data from which accurate life-related data

privacy of a person can be obtained, as well as the potential risk of seeing the commission

fraudulent acts on behalf of that person, it is a serious offence.

b) The duration of the violation: the violation lasted four days, which constitutes a duration

considerable in the light of the potential risk pointed out above.

c) The Litigation Chamber considers that the fine to be imposed and the injunction to put the

compliant processing are sufficiently dissuasive to prevent such violations at

the future.

56. The Litigation Chamber draws attention to the fact that the other criteria of article 83.2 of the

GDPR are not, in this case, likely to lead to an administrative fine other than that

defined by the Litigation Chamber in the context of this decision.

57. In its reaction to the intention to impose a fine, the Respondent objected to the amount of

the proposed fine. According to the Litigation Chamber, however, it appeared in this file

that there was a question of negligence with regard to the protection of the personal data of the

concerned person. The processing of personal data is indeed a

main activity of the defendant, hence the fundamental importance of processing personal data

staff in accordance with the GDPR.

58. The facts, circumstances and violations found therefore justify a fine that meets the

the need to have a sufficiently deterrent effect, the defendant being sanctioned with a

sufficient severity so that practices involving such offenses do not recur.

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

Litigation, this decision is published on the website of the Authority for the protection of

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

are communicated directly.

Decision on the merits 05/2021 - 21/21

60. In its reaction to the proposed fine, the Respondent asked not to publish the decision,

not even in an anonymized form. The Litigation Chamber refuses this request,

referring to the note it published on the APD website regarding the publication of

decisions, in which one can read the following: The Litigation Chamber assumes that

all of its decisions, barring exceptions, are published on its website, in a

general objective of transparency, but also of visibility and accountability."19.

FOR THESE REASONS,

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

-

to order the defendant, in accordance with article 100, § 1, 9° of the LCA, to put the

processing in accordance with Articles 5.1.f, 5.2, 24 and 32 of the GDPR, by setting

in particular the policy vis-à-vis the identification and verification of prepaid customers in

GDPR compliance. To this end, the Litigation Division grants the defendant a period

of three months and expects the defendant to report to him within the same period concerning

compliance of the processing with the aforementioned provisions.

-

pursuant to Article 83 of the GDPR and Articles 100, 13° and 101 of the LCA, to impose on the

defendant an administrative fine of 25,000 euros

for violation of articles

5.1.f, 5.2, 24, 32, 33.1 and 5, and 34.1 of the GDPR.

Pursuant to Article 108, § 1 of the LCA, an appeal may be lodged against this decision in

a period of thirty days, from the notification to the Court of Markets, with the Authority of

data protection as defendant.

(Sr.) Hielke Hijmans

President of the Litigation Chamber

19

litigation.pdf

https://www.autoriteprotectiondonnees.be/publications/politique-de-publication-des-decisions-de-la-chambre-