1/39

Litigation Chamber

Decision on the merits 56/2021 of 26 April 2021

File number: DOS-2019-02288

Subject: Complaint for unlawful consultation of personal data and refusal of right of access

The Litigation Chamber of the Data Protection Authority, made up of Mr Hielke

Hijmans, chairman, and Messrs. Yves Poullet and Christophe Boeraeve, members, taking over the business

in this composition;

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 GDPR;

Having regard to the law of 3 December 2017 establishing the Data Protection Authority (hereinafter LCA);

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

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

Considering the documents in the file;

Made the following decision regarding:

-

-

The complainant: Ms. X, represented by her counsel Maître Victor Rouard, Avenue des arts

46, 1000 Brussels,

The defendant: La Y, represented by its counsel, Maître Didier Putzeys and Me

Bernadette De Graeuwe, avenue Brigade Piron 132 in 1080 Brussels.

1. Feedback from the procedure

Decision on the merits 56/2021- 2/39

1. Having regard to the first complaint filed on April 15, 2019 by the complainant to the Authority for the Protection of

(APD), followed by a second complaint filed on April 20, 2020;

2. Having regard to the decision of April 21, 2020 of the Frontline Service of the Protection Authority

data (hereinafter “APD”) declaring the complaint admissible and the transmission of the latter to

the Litigation Chamber on the same date;

Having regard to the communication of July 31, 2020 from the Litigation Chamber informing the parties

of its decision to consider the file as being ready for substantive processing on the basis

of article 98 LCA, and the sending of the timetable for the exchange of conclusions;

3. Considering the conclusions of the defendant, received on September 8, 2020;

4. Having regard to the complainant's conclusions, received on September 30, 2020;

5. Having regard to the Respondent's summary submissions, received on October 21, 2020.

6. Having regard to the hearing of January 7, 2021 in the presence of the complainant, her counsel Me Rouard, as well as the

defendant represented by his counsel Mr De Graeuwe, as well as the DPO, Mrs Z1, and the

Compliance Officer, M.Z2;

7. Considering the sending to the parties of the minutes of the hearing and the comments of the parties;

8. Having regard to the severance of the proceedings against the plaintiff's ex-husband and against the defendant;

9. Having regard to the fine form sent to the defendant and its observations.

2. Facts and subject of the complaint

10. The complainant learned in April 2019 that twenty consultations had been made of her data at

personal character hosted in his file at the Central Individual Credit Center (hereinafter

CCP) to the Belgian National Bank (hereinafter BNB) by the defendant between 2016 and 2018.

11. The defendant is active in the financial services sector, including loans to individuals.

The ex-husband of the complainant, with whom she was in the process of leaving joint ownership following their

divorced since 2015, is employed by the defendant. The complainant argues that by consulting her

given in her file at the BNB and thus the information relating to her credits, her ex-husband

took the upper hand in joint ownership and would have caused him financial and moral damage.

12. The complainant's ex-husband also admitted having improperly consulted her data.

ci1.

13. On 14 November 2018 the complainant contacted the NBB to request the list of organizations

financiers who consulted the CCP file in his name.

14. On January 24, 2019, the plaintiff contacted the defendant to ask “what are your

criteria for consulting the National Bank files of your clients and knowing whether Y or any

other person is authorized to consult them without a specific request for funding. »

15. On February 1, 2019, the defendant's former Data Protection Officer (DPO) replied that the

CCP files “are only consulted in the context of granting or managing credits

or payment services, likely to encumber the private assets of a natural person

and whose execution can be continued (sic) on the private patrimony of this person. ".

16. However, the complainant explained that she had no open credit file with the defendant. At the time of

the hearing of January 7, 2021, the DPO of the defendant confirmed that the plaintiff has no

current file, but a closed file at home, which explains from a technical point of view

that the ex-husband was able to access the CCP file.

17. On March 13, 2019, the complainant asked what penalties were incurred by an employee who

does not comply with data protection rules. The DPO responds on March 21, 2019

requesting additional information. He offers a telephone interview in order to facilitate

Communication.

18. The complainant replied by accepting but specifying that “it is very delicate, because initially

time I do not want to harm anyone even if I have official proof”.

The telephone conversation between the defendant's new DPO and the complainant did indeed take place.

19. In an email dated April 5, 2019, the complainant reported the details of the consultations of her file to the

CCP, received from the NBB on November 14, 2018, which covers a period from April 2016 to August

2018.

1 see additional and summary submissions of the defendant p14

20. She attaches this document to her email. In this email, she accuses her ex-husband of being the author of the 20 consultations by the defendant of its file at the CCP since 2016.

21. She does not ask for confirmation of her allegations but before filing a complaint against her ex-husband, she asks for the sanctions incurred by him for having committed this intrusion into her private life.

22. On April 11, 2019, the defendant's new DPO

- responds that it does not have the elements allowing it to justify all the consultations included in the list provided by the NBB,
- confirms the rules for consulting the NBB register applicable to employees of the defendant,
- confirms the existence of disciplinary measures against employees who do not respect not these rules, and
- refuses to answer the complainant's questions about the nature of the sanction imposed on her ex-husband, in respect of the private life of SA employees.

23. On 15 April 2019, the complainant lodged a first complaint with the DPA for consultations illicit use of her data at the BNB by her ex-husband, through his duties with the defendant, and asks to be informed of the sanctions incurred by her ex-husband.

24. On September 5, 2019, the Front Line Service (“SPL”) of the APD contacted the defendant to inform it that it had been seized of a complaint by the plaintiff and requesting the legal basis and the justification for the consultation on 20 occasions, by the defendant, of the data of the complainant in the BNB's database. She also asks him to

communicate to the complainant the list of all consultations of the CCP database,

the identity of the people who consulted, as well as the data consulted.

25. On September 13, 2019, the defendant replied to the DPA:

-

that it has never approved or tolerated the consultation made by one of its employees,

data relating to the complainant in the CCP;

-

that any consultation made outside the framework of the conclusion of a credit agreement

the consumption or management thereof is prohibited;

Decision on the merits 56/2021- 5/39

-

that control measures and a disciplinary procedure exist to avoid and

punish such acts and that the author of these illicit consultations has been

sanctioned;

-

that it cannot give a legal basis, these consultations having been made outside

normal procedures, it also cannot give the names of the people

having consulted, nor the data consulted, nor communicate the list of these consultations

because the computer system does not make it possible to keep traces of the processing such

than carried out by the ex-husband of the complainant Indeed, the ex-husband of the complainant, in his capacity

executive, has different access from that of non-executive employees

("collaborators") in the register of the NBB. The technical characteristics of this system

of access prevents, according to the defendant, the conservation of any trace of the

consultations he made2.

26. On October 21, 2019, the SPL replied that it was up to the controller to ensure the security

and confidentiality of the data it collects and must respond to the request for access in accordance

in Article 15 GDPR. The complainant therefore has the right to obtain a list of the data that has been

consulted, the identity of the persons who consulted, the purpose and the legal basis. These informations

are not forwarded to the complainant.

27. On April 20, 2020 the complainant filed a new complaint with the DPA against her ex-husband and against the

defendant for abusive consultation of his personal files with the BNB via the

functions of her ex-husband within the defendant. She also asks that her ex-husband

be sanctioned in an appropriate manner and be informed of this sanction.

28. Following the severance of the proceedings, the parties were informed that the part of the complaint relating

to the complainant's ex-husband will be considered in a separate file. This decision covers

only the part of the complaint relating to the defendant.

29. The legal analysis of the complaint - corroborated by the conclusions filed by the complainant -

indicates that it raises:

- the violation of the principles of finality, loyalty, transparency, and information (articles 5,12,13,14

GDPR);

-

breach of security obligations (Article 32, combined with Articles 5.2 and 24 of the

GDPR

2 See defendant's additional and summary submissions, p.18

-

-

the lack of independence of the DPO (Article 38 GDPR);

the absence of facilitation by Y in the exercise by the plaintiff of its rights and violation

of his right of access.

30. In its submissions, the complainant invites the Litigation Division to:

-

order the defendant to send him a statement of all the consultations

of his data by the defendant (with the date, identity of the person who consulted,

legality or not of the consultation);

-

order the defendant to bring the processing of the data consulted into conformity

within the framework of its activities and send it the corrective measures implemented in order to

to ensure the security of processing;

-

impose a fine on the defendant taking into account the seriousness of the violations, the

its duration, the number of people involved, and the attitude of the defendant.

31. The defendant refutes the complaints.

3- As to the reasons for the decision

I- On the competence of the DPA

32. Pursuant to Article 4.1 LCA, the DPA is responsible for monitoring the principles of protection

data, as affirmed by the GDPR and other laws containing provisions relating to the

protection of the processing of personal data.

33. Pursuant to Article 33.1 LCA, the Litigation Chamber is the litigation body

administration of ODA3. It receives complaints that the SPL transmits to it pursuant to Article

62.1 LCA, i.e. admissible complaints when, in accordance with article 60 paragraph 2 LCA, these

complaints are written in one of the national languages, contain a statement of the facts and the

indications necessary to identify the processing of personal data on which

they relate to and come under the competence of the APD.

34. Pursuant to articles 51 and s. of the GDPR and Article 4.1 LCA, it is up to the Chamber

Litigation as an administrative litigation body of the DPA, to exercise effective control

the application of the GDPR and to protect the fundamental rights and freedoms of individuals

3 The administrative nature of the litigation before the Litigation Chamber was confirmed by the Court of

markets, jurisdiction of appeal of the decisions of the Litigation Chamber. See. in particular the judgment of June 12, 2019,

published on the APD website, as well as decision 17/2020 of the Litigation Chamber.

Decision on the merits 56/2021- 7/39

with regard to the processing and to facilitate the free flow of personal data within

within the Union.

35. As the Litigation Chamber has already had occasion to state4, data processing

are operated in multiple sectors of activity, particularly in the professional context such as

in the present case. The fact remains that the competence of ODA in general, and of the

Litigation Chamber in particular, is limited to monitoring compliance with the regulations

applicable to data processing, regardless of the sector of activity in which these

data processing takes place. Its role is not to replace the courts of the order

judiciary in the exercise of their powers. Therefore, as the defendant

further notes in its conclusions, the Litigation Division is not competent to

rule on the content of the disciplinary sanction imposed by the defendant on the former husband of

the complainant, following the illicit consultations he carried out. However, according to article

51 GDPR, the DPA remains competent to verify the effectiveness of the organizational measures

put in place in the event of violation of the provisions of the GDPR, in particular those relating to the

treatment safety. To this extent, the DPA reserves the right to obtain communication

by the defendant of the nature of the disciplinary sanction imposed on the complainant's ex-husband,

as well as any other measure put in place to prevent further unlawful processing by the

employees of the defendant.

36. As indicated above, following the decision of the Litigation Division to sever the proceedings,

this decision does not examine the part of the complaint relating to the complainant's ex-husband, but

only the part relating to the defendant. To the extent that the defendant is active in

the banking sector and processes large volumes of sensitive financial data, and taking

considering that it is part of a multinational with more than 10,000 employees in

Belgium , as well as in view of the fact that the effective exercise of the rights of data subjects (including

the right of access) is one of the thematic priorities of the APD5, the Litigation Chamber considers

appropriate to examine this aspect of the complaint as a matter of priority.

37. The Chamber also notes that the conflict between the complainant and her ex-husband is linked to the divorce between

them and when they leave joint ownership, aspects which do not fall under the right to data protection.

38. For the rest, the Litigation Chamber notes that if it is not competent for the

illicit consultations having taken place before May 25, 2018, the date of entry into force of the GDPR, it

good for later consultation. To the extent that the consultations have extended

until August 2018, the Litigation Chamber is fully competent.

4 See. in particular decision 03/2020 of the Litigation Chamber.

5 See the ODA priorities for 2019-2025 in its Strategic Plan, published on the site.

II- On the merits

II.1- Regarding the status of controller and processor

II.1.1- Definitions and status of controller and processor

39. In accordance with Article 4.7 of the GDPR, the person responsible for the

processing: "the natural or legal person, public authority, agency or other body

who, alone or jointly with others, determines the purposes and means of the processing. »

40. Article 4.8 of the GDPR stipulates that it is necessary to consider as the processor: “the person

physical or legal entity, public authority, service or other body which processes data

of a personal nature on behalf of the controller. »

41. The Data Protection Authority has also specified the following aspects on the quality of

subcontractor: “The existence of subcontracting depends on the data controller who must

have decided not to carry out the processing themselves for which they control the purpose(s) and/or

means but to delegate all or part of the operations to another person or

external organization than his own. This other person must be legally distinct from

the organization of the data controller and must carry out the processing operations of

personal data delegated on behalf of the latter and in accordance with its

documented instructions. 6 (emphasis added).

42. In accordance with Guidelines 07/2020 of the EDPB7, the Litigation Chamber assesses

specifically the role and quality of the data controller(s) concerned.

43. In this case, the Litigation Division finds that it is indeed the defendant who determines

the purposes and means of the processing. Indeed, the consultations of the CCP of the BNB are

carried out solely within the framework of the granting of credit to individuals or in the management of

these files. It is also the defendant who provides the means to carry out this

processing (through its IT systems). It should therefore be considered responsible.

treatment.

6 Note from the DPA "Update on the notions of controller / processor with regard to the Regulation

(EU) n° 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data

personnel (GDPR) and some applications specific to liberal professions such as lawyers", September

2018, p 2.

7 EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 02 September 2020, point

12.

44. It should nevertheless be emphasized from the outset that, as recalled by the CJEU in its judgment

Wirtschaftsakademie of June 5, 2018, "the notion of "controller" refers to the organization

which, "alone or jointly with others", determines the purposes and means of the processing

of personal data, this concept does not necessarily refer to an organization

unique and may concern several actors (…)"8. That the defendant is responsible for

treatment for the consultations of its employees in the CCP register does not therefore mean, in the

case in point, that it alone corresponds to this quality. It is indeed necessary to distinguish the

consultations in the CCP register in the context of the purposes of the defendant (granting or management of

credits), abusive consultations carried out for private purposes by the complainant's ex-husband.

As indicated below, although he used the means made available to him by the

defendant, insofar as the defendant's ex-husband carried out the disputed consultations

outside the scope of his duties as an employee of the defendant, he must be considered

as data controller for these abusive consultations specifically.

45. As the EDPB indicates, this nevertheless in no way exempts the defendant, as

responsible for processing, consultations in the CCP register, its obligation to ensure the

processing security9. This aspect is developed below (see II.1.2- On the responsibility of the

controller).

46. With regard to the status of subcontractor, the Litigation Chamber considers that the complainant

cannot be followed in its argument that the plaintiff's ex-husband is underprivileged.

dealing with the defendant. Indeed, the two conditions mentioned above are not met.

The complainant's ex-husband, as an employee, is not a separate legal entity from the

defendant, and he did not carry out the processing on behalf of and on the basis of the instructions of

the defendant.

47. Therefore, the complaint of non-compliance with the obligations relating to subcontracting (Article 28 GDPR) as

that developed by the complainant is irrelevant, and is not considered further in the context

of this decision.

II.1.2- On the responsibility of the data controller

8 CJEU, case. C 210/16, 5 June 2018, ECLI:EU:C:2018:388, §29.

9 Opinion 1/2010 on the notions of “controller” and “processor”, WP169, p.17.

48. The defendant refers to Opinion 1/2010 of the Group 29 on the notions of “responsible for the

processing” and “processor”10, to affirm that it is not responsible for processing and

that this quality must be recognized in the head of the complainant's ex-husband.

49. The Chamber emphasizes the following passages from this opinion (pp. 16-19):

“From the strategic perspective of assigning responsibilities, and so that people□

concerned can turn to a more stable and reliable entity when exercising the rights□

conferred on them by the directive, it would be preferable to consider as responsible for the□

treats the corporation or organization as such, rather than a person within it. It's in□

effect the company or organization that should be considered, in the last resort, as responsible□

data processing and obligations set out in data protection legislation□

data, unless certain specific elements indicate that a natural person must□

to be responsible.□

In general, it will be assumed that a company or a public body is□

responsible as such for the processing operations that take place in his domain□

activities and risks.□

50. Sometimes companies and government agencies designate a specific person to be□

responsible for carrying out processing operations. However, even when a person□

physical is appointed to ensure compliance with data protection principles or to□

process personal data, it is not responsible for the processing but acts for□

the account of the legal entity (company or public body), which remains liable in the event□

breach of the principles, in its capacity as controller. (emphasis added)□

51. The defendant refers more specifically to the following paragraph of the opinion:□

“A separate analysis is required where a natural person acting within a□

legal person uses data for personal purposes, outside the framework and the possible□

control of the activities of the legal person. In this case, the natural person in question would be□

decided data controller, and would assume responsibility for such data use□

of a personal nature. The initial processing manager could nevertheless keep a□

some degree of responsibility if the new processing took place due to a lack of□

security measures. »□

10 Opinion 1/2010 on the notions of "controller" and "processor", WP169, p.17.□

52. The Litigation Chamber underlines the following part of the same opinion:

“To sum up the considerations which have just been set out, it appears that the person responsible

in the event of non-compliance with data protection is always the controller, except

namely the legal person (company or public body) or the physical person formally

identified according to the criteria of the directive. If a natural person working in a company

or a public body uses data for personal purposes, outside the activities of the

company, it must be considered as a de facto data controller and assume the

criminal liability as such. (p18) (emphasis added)

53. The Working Group similarly cites an example:

“Example #4: Secret Surveillance of Employees

A member of the board of directors of a company decides to secretly monitor the

employees of the company, while this decision has not officially received the approval of the board

administration. The company must be considered the data controller and face

to any complaints and lawsuits by employees whose personal data

have been misused.

The legal liability of the company is due in particular to the fact that as

responsible for the processing, it has the obligation to guarantee compliance with the security rules

and confidentiality. Misuse by a company officer or employee

could be considered the result of inappropriate security measures.

In this respect, it is important that the member of the board of directors or other natural persons

in society are subsequently held liable, both in civil matters (also

towards society) than penal. This could in particular be the case if the board member has

used collected data to obtain personal favors from employees: he should then

be considered as a "controller" and be held liable for this

use of data. » (p18-19)

54. This Opinion 1/2010 has been superseded by Guidelines 07/2020 of the EDPB (successor to the

Group 29), according to which:

“Whereas the terms “personal data”, “data subject”, “controller” and “processor” are defined in

the Regulation, the concept of “persons who, under the direct authority of the controller or

processor, are authorized to process personal data” is not. It is, however, generally understood

Decision on the merits 56/2021- 12/39

as referring to persons that belong to the legal entity of the controller or processor (an employee

or a role highly comparable to that of employees, e.g. interim staff provided via a temporary

employment agency) but only insofar as they are authorized to process personal data.”11

(free translation:

55. While the terms 'personal data', 'data subject', 'data controller'

processing" and "processor" are defined in the Regulation, the notion of "persons who, under

the direct authority of the controller or processor, are authorized to process

personal data" is not. However, this concept is generally understood

as referring to persons who belong to the legal entity of the person responsible for the

processor or processor (an employee or role highly comparable to that of

employees, e.g. temporary staff provided through an employment agency

temporary) but only insofar as they are authorized to process personal data.

personal character".)

56. A careful reading of the notice shows that, conversely, an employee who does not have access within the framework

of his functions to personal data, which he would use for his own purposes, must be

considered as a third party, i.e. as an entity distinct from his employer:

57. "An employee etc." who obtains access to data that he or she is not authorized to access and for

other purposes than that of the employer does not fall within this category. Instead, this employee

should be considered as a third party vis-à-vis the processing undertaken by the employer. Insofar

as the employee processes personal data for his or her own purposes, distinct from those of his

or her employer, he or she will then be considered a controller and take on all the resulting

consequences and liabilities in terms of personal data processing".12

(free translation:

58. An employee, etc. who obtains access to data to which he is not authorized to access and to

purposes other than those of the employer does not fall into this category. This employee must

rather be considered as a third party vis-à-vis the processing carried out by the employer. In the

to the extent that the employee processes personal data for his own purposes, separate

those of his employer, he will then be considered responsible for the processing and will assume

all the consequences and responsibilities arising therefrom in terms of data processing

personal.)

11 Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2 September 2020, point 86, p27

12 Ibid.

59. In the present case, although the complainant's ex-husband had access to the CCP on the basis of his

mission of control of the credit files, the disputed consultations were carried out outside

of his duties as an employee. It is appropriate to follow the reasoning adopted by

the EDPB in the Guidelines 07/2020, and therefore to consider the ex-husband as

separate third party from the defendant for abusive consultations specifically.

60. The defendant must therefore be followed in its argument that the ex-husband is responsible

of treatment for abusive consultations.

61. The Chamber nevertheless notes that the liability of the ex-husband is not examined in the

present decision, but only that of the defendant, insofar as the procedures

to these two parties have been severed.

62. The Chamber therefore distinguishes the processing carried out in the context of consultations of the CCP register

as provided for by the purposes of the defendant, abusive consultations carried out by

the complainant's ex-husband. Although the latter is responsible for processing for consultations

abusive, the defendant remains responsible for processing for consultations in the CCP register

within the framework of the purposes it determines (granting or management of loans to individuals). In

In this context, it remains subject to the principle of responsibility (articles 5.2 and 24 GDPR) as

controller and employer, as well as Articles 29 GDPR13 and 32 GDPR, in particular

in its paragraph 414.

63. Insofar as it is the responsibility of the data controller to guarantee the security of the processing

(including access to data in accordance with the GDPR by its employees), it was up to the

defendant to implement the appropriate technical and organizational measures to avoid

abusive treatment by its employees, as in the present case (this aspect is developed below).

This is all the more applicable in view of the sensitive nature of the data to which the

employees of the defendant have access (financial data). This position is also the one

defended in the doctrine.

13 Article 29 GDPR: “The processor and any person acting under the authority of the controller or

under that of the subcontractor, who has access to personal data, cannot process this data,

except on instructions from the controller, unless required to do so by Union law or by

of a Member State"

14 Article 32.4 GDPR: “The controller and the processor shall take measures to guarantee

that any natural person acting under the authority of the controller or the processor,

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

processing, unless required to do so by Union law or the law of a Member State. »

15 Delforge, A., “Title 8 - The general obligations of the controller and the place of the processor”

in General Data Protection Regulation (RGPD/GDPR), Brussels, Éditions Larcier, 2018, p. 374

64. If, conversely, and as argued by the defendant, the employer should be exempted from any

security liability for the irregular treatment of its employees carried out within the framework

of their functions, even for their own purposes, this would remove part of its useful effect from the GDPR

and the protection of personal data.

65. The Chamber nonetheless emphasizes that regardless of who is responsible

of treatment for abusive consultations, it is the obligation of the defendant in its capacity

as data controller to ensure the security of data and processing which constitutes

the heart of this decision. In the present case, the defendant does not dispute its obligation

to ensure the security of access by its employees to the CCP register and more generally to the data

of the BNB. This aspect will be developed below.

II.2- As for the principle of responsibility and the obligation to ensure the safety of

personal data

II.2.1- Principle of responsibility

66. Article 24.1 GDPR states that “taking into account the nature, scope, context and

purposes of the processing as well as the risks, the degree of probability and severity of which varies, for

the rights and freedoms of natural persons, the controller implements the

appropriate technical and organizational measures to ensure and be able to

demonstrate that the processing is carried out in accordance with this Regulation. These measures are

reviewed and updated as necessary. ". This article translates the principle of responsibility, or

of “accountability” set out in Article 5.2. GDPR, according to which "The controller is

responsible for compliance with paragraph 1 and is able to demonstrate that it is complied with

(responsibility). »

67. Section 24.2. of the GDPR specifies that when this is proportionate with regard to the activities of

processing, the measures referred to in Article 24.1. of the GDPR above include the implementation

implementation of appropriate data protection policies by the data controller

processing.

68. Recital 74 of the GDPR adds that “There is a need to establish the liability of the data controller

processing for any processing of personal data that it carries out itself or that

is carried out on his behalf. In particular, it is important that the controller is required

to implement appropriate and effective measures and be able to demonstrate the
compliance of processing activities with this Regulation, including the effectiveness of
measures. These measures should take into account the nature, scope, context and
Decision on the merits 56/2021- 15/39
purposes of the processing as well as the risk that this presents for the rights and freedoms of
physical persons ".

69. It is also his responsibility, pursuant to Article 25 of the GDPR (data protection from the
design and by default), to integrate the necessary compliance with the rules of the GDPR upstream of its
acts and procedures (for example, ensuring the existence and effectiveness of control procedures
for employees but also managers in their access to CCP data).

70. In addition, the data controller is required, on the basis of Article 32 GDPR, to ensure the
security of processing, "taking into account the state of knowledge, the costs of implementing
and the nature, scope, context and purposes of the processing as well as the risks, including
the degree of likelihood and severity varies, for the rights and freedoms of natural persons".

However, the Litigation Chamber notes a lack of respect for the obligation to ensure the security
treatment on the part of the defendant, which forms part of the principle of responsibility. This
breach is developed below.

71. This breach of the obligation to ensure the security of processing constitutes the anchor point of
this Decision and the penalties it imposes. The absence of technical measures and
organizational measures to limit unjustified and insufficiently secure access by a
employed in the NBB's CCP database, and a fortiori the absence of an ex
post about the accesses that have taken place, is considered a serious violation. The executive position
occupied by this employee cannot justify this lack of security measures.

II.2.2-The personal data security obligation and the logging of IT logs

a- The contours of the safety obligation

72. On the basis of Article 5.1.f) GDPR, personal data must be processed in a manner

to ensure appropriate security, “including protection against unauthorized processing or illicit and against accidental loss, destruction or damage, using measures appropriate techniques or organisational. In the absence of appropriate measures to secure the personal data of the persons concerned, the effectiveness of the rights fundamental to privacy and the protection of personal data cannot be guarantee16, a fortiori in view of the crucial role played by information and communication in our society.

16 The crucial role played by data security for the effective exercise of their rights by individuals concerned was enshrined in particular by the ECHR in its judgment of 17 July 2008, I. c. Finland, req. no. 20511/03, in which the Court unanimously finds a violation of Article 8 by the Finnish authorities,

73. As indicated above, the breach of the obligation to ensure the security of processing constitutes the heart of decision. The impact in terms of respect for the right to protection of the private life of the complainant linked to the absence of technical and organizational measures to limit unjustified and insufficiently secure access by an employee to the CCP database of the BNB is also reinforced by the lack of possibility of ex post traceability of consultations operated. The Litigation Chamber recalls that the combined reading of Articles 32 (obligation to ensure the security of processing), as well as 5.2 and 24 GDPR (subjecting the person responsible for the processing to the principle of accountability) requires the controller to demonstrate its compliance with Article 32, by taking appropriate technical and organizational measures, transparent and traceable way. Keeping a log of IT logs, or “logging” revolves around these obligations, more particularly the traceability of processing, and contributes to the necessary “availability”17 of the data processed.

74. The Litigation Chamber also recalls the provisions of Article 25 (data protection from the design and by default), which requires the data controller to integrate the necessary compliance with the rules of the GDPR upstream of its acts and procedures (for example, ensuring

the existence and effectiveness of control procedures for employees but also managers

in their access to CCP data).

75. It should be noted that the principle of security with its various components of integrity,

confidentiality18 and availability19 is included in articles 5.1.f) and 32 of the GDPR and is now

elevated in the GDPR to the same rank as the fundamental principles of lawfulness, transparency and

loyalty.

76. The obligations of data controllers with regard to the security of processing are based on

GDPR Articles 32 et seq.

77. The classic components of recommendations in terms of information security, such as

recommended by ISO27xxx20 are the confidentiality of data, their integrity and their

on the basis of insufficient protection against unauthorized access to a nurse's medical file

seropositive.

17 Article 32.1.a GDPR

18 According to the Group 29, data integrity corresponds to “the quality by virtue of which the data are

authentic and have not been inadvertently or maliciously altered during processing, storage or

transmission. The notion of integrity can extend to computer systems and requires that the processing of

personal data on these systems remains unaltered” Group 29, WP 196, Opinion 05/2012 on Cloud

Computing, p. 18.

20 The ISO27xxx suite of standards is one of the main international information security standards.

availablity. Added to these is the notion of imputability, “which makes it possible to identify, for

all actions performed, people, systems or processes that initiated them

(identification) and to keep track of the perpetrator and the action (traceability)”21.

78. Accountability is expressed in particular in a concrete way by keeping a register of log files.

79. Logging therefore consists of the recording of relevant information concerning the

events of a computer system (access to the system or to one of its files, modification

of a file, data transfer, etc. in files called “log files”. Information

occasions are, among other things, the data consulted, the date, the type of event, the data

identifying the author of the event, as well as the reason for this access. This allows

in particular to identify any consultation of abusive personal data or for a purpose

not legitimate, or to determine the origin of an accident.

80. Although logging is not expressly mentioned in the GDPR22, the keeping of a

journal of log files constitutes a technical and organizational measure envisaged in the article

32 GDPR. It constitutes good practice, recommended by the Litigation Chamber at all

data controller. These measures must be adapted to the risks.

81. The predecessor institution of the DPA (the Privacy Commission; hereinafter the OPC) already indicated

in its Personal Data Information Security Guidelines23

as well as in its Recommendation24 to cities and municipalities25 concerning log registers

21 Dumortier, F., “Chapter 4 - Cybersecurity, privacy, accountability, logging and log files” in Les obligations

legal cybersecurity and incident notification, Brussels, Politeia, 2019, p. 187 and APD, “Note on

the security of personal data”, p2.

22 Conversely, Directive (EU) 2016/680 attaches particular importance to the consultation and disclosure

(the most common treatment). and imposes the identification of the author of the treatment as well as that of the recipients

in the event of disclosure, the exact moment, as well as the justification of the processing (of April 27, 2016 relating to the

protection of natural persons with regard to the processing of personal data by the authorities

authorities for the purposes of the prevention, detection, investigation and prosecution of criminal offences.

matter or execution of criminal penalties, and on the free movement of such data).

23 Available on the link https://www.autoriteprotectiondonnees.be/publications/lignes-directrices-pour-la-

information-security.pdf.

24 Recommendation to towns and municipalities concerning the recording of the reason for consulting the Register

by their staff members (CO-AR-2017-013), August 30, 2017, p7

25 In this recommendation to cities and towns concerning logging, the CPP emphasizes the importance

of logging as an "essential element of any information security policy" and indicates:

“21. The development of an adequate information security policy is necessary in order to take

measures which exclude any unauthorized access, and this in a documented manner allowing the municipality

to assume its responsibility. In its benchmark security measures applicable to any processing

of personal data, the Commission has already stressed that the establishment of a selective mechanism

research and logging is an essential element of any security policy for

information. (…) these guidelines prescribe that all access to the computer system must be traceable in order to

to verify who had access, when, to what and for what reason.

(…)

Decision on the merits 56/2021- 18/39

IT that logging is an essential part of any IT security policy.

information, in that it allows the traceability of access to computer systems26.

b- Link between the security obligations of data controllers and the principles of

accountability and transparency

82. The Litigation Chamber recalls that Article 32 GDPR must be read in conjunction with Article

5.2 GDPR and the aforementioned Article 24 GDPR, subjecting the controller to the principle of

responsibility. It is the controller's responsibility to demonstrate compliance with the provisions

of the GDPR, by taking appropriate technical and organizational measures, in a way

transparent and traceable, allowing in the event of an inspection to provide proof of the guarantees

applied.

83. The principle of accountability, read in conjunction with the principle of transparency (Article 5.1.a

GDPR), allows data subjects to exercise their rights and monitor the compliance of

processing carried out on their personal data. It thus makes it possible to assume the

responsibility27.

84. Recital 63 of the GDPR further adds to this that this right of access must be considered as

a control mechanism: "A data subject should have the right to access the data

personal data that have been collected about him and to exercise this right easily and at

reasonable intervals, in order to become aware of the processing and to verify its lawfulness."

85. These principles of accountability and transparency are articulated with Article 15 of the GDPR, which

guarantees the data subject's right of access to their personal data processed. The CPP

already concluded with regard to journaling, unequivocally:

86. “An incomplete log file and no mention of the reason for the consultation

constitute an infringement of the useful exercise of the right of access and control available to the person

concerned. This also compromises the exercise of other rights such as the right of rectification

23. Finally, the Commission itself has already indicated on several occasions that recording the reason for the

consultation of the National Register is of crucial importance. In its recommendations on the management

access and users in the public sector and to the communication of information contained in the

population registers, the Commission stresses the importance of full tracing (who, what, when, why)

implying a logging of each consultation of the population registers, so that any

consultation of data for a non-legitimate purpose or for personal purposes can be detected and sanctioned.

By extension, this obligation is also valid for consulting and updating the National Register. » (p8)

(the Chamber underlines)

26 Although this recommendation is addressed to municipalities and towns, the reasoning applies to other types

data processing, especially when it comes to sensitive data.

27 See recital 78 GDPR.

(Article 16 of the GDPR), the right to be forgotten (Article 17 of the GDPR), and the right to restriction of use

of data processed unlawfully (Article 18 of the GDPR). »28 (p. 10) (emphasis added)

87. The Litigation Chamber recommends keeping a log register of the log files in

as a good practice, since logging is useful for everything

controller, in that it ensures the materialization of the

principle of availability, itself closely linked to the principles of confidentiality and

data integrity.

88. As indicated above, the effectiveness of the fundamental rights to privacy and the protection of

personal data depends significantly on the measures put in place to ensure

the security of these29, the keeping of a register of logs, although not imposed as such by the

GDPR, is therefore encouraged by the Litigation Chamber.

89. This applies a fortiori to credit institutions, insofar as the law imposes on them a

consultation of the credit status of the persons concerned at the NBB before granting a loan.

II.2.3- Application to the present case

90. In the light of the foregoing, and particularly insofar as the consultation of the data

personal information relating to the credits of the persons concerned constitutes an invasive processing of

sensitive financial data, the Litigation Chamber considers that the measures put in place

must be all the more adapted as the risks for the fundamental rights of individuals

concerned are high.

91. The importance of these risks as a factor is highlighted in several relevant articles of the

GDPR, including Articles 24, 25 and 32.

92. However, in the present case, an employee of the defendant was able to carry out on 20 occasions

illicit consultations of this sensitive financial data, over a period extending from April 2016

to August 2018.

28 Recommendation to towns and municipalities concerning the recording of the reason for consulting the Register

by their staff members (CO-AR-2017-013), August 30, 2017, p10. Along the same lines, see

decision of the Sectoral Committee of the National Registry of 11/01/2012.

29 Dumortier, F., “Chapter 4 - Cybersecurity, privacy, accountability, logging and log files” in Les obligations

legal cybersecurity and incident notifications, Brussels, Politeia, 2019, p 141

93. This, combined with the absence of keeping an access log register or any control

access by executives (including the ex-husband) to the registers of the BNB by the defendant

before the incident, demonstrates the insufficiency of the measures on the part of the defendant.

94. During the hearing, although she pointed out the existence of a log of the accesses of the non-executive employees as well as the ethical regulations prohibiting any use abuse of access, the defendant's DPO confirmed the absence of any system of executive access control.

95. This constitutes a flagrant violation of Article 32 GDPR (security of processing), read in combination with Article 5.2 GDPR and Article 24 GDPR.

96. This lack of logging or other security measures on the part of the defendant also prevents the complainant from being able to exercise her right of access concerning the processing unlawful acts carried out by her ex-husband, an employee of the defendant, since the defendant keep no trace.

97. The DPA SPL indeed asked the defendant in its letter of 5 September 2019 to communicate to the complainant the list of consultations and the data concerned, as well as the identity of the author of these consultations.

98. This aspect of exercising the right of access is developed below (see point II.4).

99. The defendant further argues that “numerous measures have been put in place (…) in order to reduce as much as possible the risk of illegitimate consultations of the Central Credit to Individuals by members of its staff”.30

100. It refers to these measures, and argues that they were reinforced following the abusive consultation by the complainant's ex-husband.

101. She quotes as follows:

•

selection of personnel on the basis of good repute and training of personnel relating to the security (including a review for employees with access to data from the CCP);

•

technical limitations for access to CCP data:

30 Defendant's additional and summary submissions, p12.

Decision on the merits 56/2021- 21/39

o a credit file must exist;

oh

if access via the system reserved for non-executive employees, consultation and

the employee's identity is recorded;

oh

if access via the CCP website (reserved for executives), this access is only

possible via the executives' computers, and a username and password (unique

for all SA executives) is required;

•

human controls at several levels.

102. The fact remains that the complainant can be followed when she notes that the

defendant admits in its conclusions that for its executives, while they have access

extended to the data in the CCP certainly for the following purposes only: "corrections to be made

in the data encoded in the CCP, the consultation of the contact details of the mediator in the event of

collective debt settlement, and the operation called “clean BNB”, namely the comparison of

data included in the CCP with the defendant's files”31.

103. There is no data consultation control system at the PCU.

104. The defendant itself specifies in this regard that for executives, it is impossible to identify

the specific person who viewed the data.

105. The defendant moreover recognizes this implicitly when it argues that since the

illicit consultations denounced by the complainant, a series of additional measures were

put in place within the company (including GDPR training for managers, strengthening of

front-line controls (i.e. non-managerial employees).

106. Especially vis-à-vis the executives, the defendant's DPO, questioned during the hearing on the security measures taken specifically concerning executives' access to the NBB registers since the incident, explains that access is now limited to two supervisors (instead of five as before), and the password has been changed twice (once in 2019 and once in 2020).

107. It adds that the defendant asked the BNB at the end of 2020 (therefore recently) to provide him with his own list of accesses in order to be able to compare it with the list kept by the two executives having access to the registers of the NBB, in order to identify any differences in a goal of controlling the activity of executives

31 Additional and summary conclusions p10.

108. The Litigation Division takes note of the efforts made, which moreover remain in its view insufficient as regards executives having access to the registers of the NBB, without that this influences the breach of its security obligation – in accordance with the principle of liability - on the part of the defendant.

109. It also notes that no evidence of these additional measures has been provided to it.

110. The defendant further notes that each year it carries out tens of thousands of CCP consultations in all lawfulness, and that the number of illicit consultations is limited to 20, spread between April 2016 and August 2018.

111. The Litigation Chamber takes note of this, but recalls that this does not detract from the consultations their illicit or repeated nature, to sensitive personal financial data.

112. The Litigation Chamber finds that the defendant was and remains in default of bringing implement the appropriate technical and organizational measures required by article 24.1 and 2 of the GDPR to guarantee not only data security by avoiding illicit consultations, but also an effective exercise of the rights of the persons concerned such as the complainant in lack of logging.

113. The defendant also points out that the complainant for the first time referred to

an “intrusion” with her 7 months after the last illicit consultation, although she was

already informed for 4 months. This is irrelevant, as the plaintiff is free

to exercise their rights at any time.

114. The defendant therefore violated Article 32, read in conjunction with Articles 5.2 and 24 of the GDPR.

II.3- Regarding compliance with the principles of finality, transparency and information

II.3.1- On the principles of loyalty, transparency and information

115. Pursuant to Article 5.1, a), personal data must be

"processed

in a lawful, fair and transparent manner with regard to the data subject (lawfulness, fairness,

transparency)”.

116. In addition, pursuant to Articles 13 and 14 of the GDPR, any person whose data to

personal character are processed must, depending on whether the data is collected directly from

Decision on the merits 56/2021- 23/39

from it or from third parties, to be informed of the elements listed in these articles (§§ 1 and 2)32. In case of

direct collection of data from the data subject, the latter will be informed of both the

elements listed in article 13.1 and 2 of the GDPR, i.e.:

• the identity and contact details of the data controller as well as the contact details of the

potential data protection officer

• the purposes of the processing as well as the legal basis thereof (when the processing is

based on the legitimate interest of the data controller, this interest must be specified)

• recipients or categories of recipients of the processing

• the intention of the data controller to transfer the data outside the Space

European Economic

• the data retention period,

• the rights conferred on him by the GDPR, including the right to withdraw his consent to any

when and when to lodge a complaint with the data protection supervisory authority.□

data (in this case ODA□

• information on whether the requirement to provide personal data□

staff is of a regulatory or contractual nature and the consequences of their non-□

provision as well as the existence of automated decision-making including a□

profiling, referred to in Article 22 of the GDPR.□

117. The Litigation Chamber also recalls that in the event of direct collection (Article 13 of the GDPR),□

no exceptions are provided.□

118. Articles 14.1 and 2 list elements which are similar taking into account however that the hypothesis□

referred to in Article 14 of the GDPR is that where data is not collected directly from□

of the person concerned but indeed with third parties.□

119. This information is, whether on the basis of Article 13 or Article 14 of the GDPR to be provided□

to the data subject in compliance with the procedures set out in Article 12 of the GDPR.□

II.3.2- The complainant's position regarding the application of the principles of loyalty, transparency and□

information□

32 In the guidelines it devoted to the principle of transparency (point 13), the Group 29 thus states□

: “(…) the position of the G29 is that there is no difference between the status of the information to be provided under the□

paragraph 1 and paragraph 2 of Articles 13 and 14, respectively. All the information contained in□

these paragraphs are of equal importance and must be provided to the data subject”. Bedroom□

Litigation endorsed this position in particular in its decision 41/2020 (p19).□

Decision on the merits 56/2021- 24/39□

120. The complainant points out that the defendant, when it became aware through its exchanges with□

the plaintiff of the illicit consultations carried out by its employee, moreover recognized by□

the latter, refrained from providing him with the vast majority of information under Article 14□

GDPR. It thus indicated to him the purpose of the processing (consultation of the data at the CCP under□

of its legal obligation and within the framework of the management of credit agreements), but did not□

sends its Privacy Policy. For example, it did not inform the complainant

the data retention period.

121. The fact that the complainant was already in possession of the list of consultations (obtained

via the BNB), does not change the finding that the defendant did not provide it with the other

information required under Article 14, which it was able to provide.

122. II.3.3- The position of the defendant regarding the application of the principles of fairness, transparency

and information

123. The defendant first argues that the complainant requested the information from the

title of article 14 in its conclusions for the first time, and would never have expressed this

request in the exchanges between parties before. The Litigation Chamber is of the opinion that

this is in bad faith, insofar as the SPL of the APD has formally requested the

defendant33 to transmit this information to the complainant, a request which remained unanswered.

124. Furthermore, Article 14.3 of the GDPR indicates:

“The controller shall provide the information referred to in paragraphs 1 and 2:

(a)within a reasonable period of time after obtaining the personal data, but no longer than

not a month, having regard to the particular circumstances in which the personal data

staff are processed;

b) whether the personal data is to be used for the purposes of communication with the

data subject, at the latest at the time of the first communication to that person; Where

(c) if it is intended to communicate the information to another recipient, at the latest when the

personal data is communicated for the first time”. (emphasis added)

33 Letter of 21 October 2019 from the SPL.

125. The data controller must therefore transmit the information required on his own

initiative, instead of waiting for the request to be made by the data subject. In this case,

insofar as the personal data were to be used for the purposes of the

communication with the complainant, this information should have been sent to her no later than

at the time of the first communication between the parties.

126. The defendant then attempts to absolve itself of liability, by repeating its argument that

it is not responsible for the treatment for the illicit consultations of the data of the

complainant, and that the obligation to provide the information under Article 14 GDPR would fall

to her ex-husband.

127. As indicated above, this reasoning cannot be followed.

128. The defendant is indeed bound by the principle of transparency and information (Article

14 GDPR in this case), fundamental article laying down clear and essential obligations with regard to

data controllers to enable data subjects to exercise their rights.

129. In addition, the defendant explains that no trace is kept within the framework of the system of

consultation of data at the CCP reserved for supervising executives, such as the ex-husband of the

complainant, and that it is therefore materially unable to provide information as to the

data consulted.

130. The Litigation Division is of the opinion that this constitutes an admission, as indicated above, of

defendant's breaches of the principles of liability and security (Articles 5.2, 24

and 32 GDPR).

131. The arguments put forward by the defendant to get rid of its obligation to respect the

principles of loyalty, transparency and information cannot be retained.

132. Consequently, and since the defendant does not demonstrate that the information that the

defendant was in a position to provide (despite the advanced technical impossibility of providing

the list of data consulted for example) under Article 14 would have been transmitted to the

plaintiff, the Litigation Chamber concludes that the defendant failed in its obligation

information about it.

133. The Litigation Chamber recalls that an essential aspect of the principle of transparency

in light of Articles 12, 13 and 14 of the GDPR is that the data subject should be in

able to determine in advance what the scope and consequences of the processing encompass

Decision on the merits 56/2021- 26/39

so as not to be caught off guard at a later stage as to how his data to

personal character were used.

134. Information should be concrete and reliable, it should not be formulated in

abstract or ambiguous terms or leave room for different interpretations. More

in particular, the purposes and legal bases of the processing of personal data

staff should be clear.

II.4- Regarding the facilitation of the rights of the complainant and her right of access

135. Article 12 of the GDPR states:

"1. The controller shall take appropriate measures to provide any information

referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22

and Article 34 with regard to the processing to the data subject in a concise manner,

transparent, understandable and easily accessible, in clear and simple terms, in particular

for any information intended specifically for a child. Information is provided in writing

or by other means including, where appropriate, electronically. When the person

concerned so requests, the information may be provided orally, provided that

the identity of the data subject is demonstrated by other means.

2. The controller shall facilitate the exercise of the rights conferred on the data subject at

under Articles 15 to 22. In the cases referred to in Article 11(2), the controller

does not refuse to comply with the data subject's request to exercise the rights

confer Articles 15 to 22, unless the controller demonstrates that it is not

able to identify the data subject. (emphasis added)

136. Article 15 GDPR stipulates:

"1. The data subject has the right to obtain from the controller confirmation that

personal data concerning him are or are not processed and, when they are,

access to said personal data as well as the following information:

a) the purposes of the processing;

(b) the categories of personal data concerned;

Decision on the merits 56/2021- 27/39

c) the recipients or categories of recipients to whom the personal data have been

or will be communicated, in particular recipients who are established in third countries or

International organisations;

d) where possible, the envisaged retention period of the personal data

or, where this is not possible, the criteria used to determine this duration;

e) the existence of the right to request from the controller the rectification or erasure of

personal data, or a restriction on the processing of personal data

relating to the data subject, or the right to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) when the personal data is not collected from the data subject,

any information available as to their source;

h) the existence of automated decision-making, including profiling, referred to in Article 22,

paragraphs 1 and 4, and, at least in such cases, useful information concerning the underlying logic

underlying, as well as the importance and the expected consequences of this processing for the person

concerned.

2. When the personal data is transferred to a third country or to a

international organization, the data subject has the right to be informed of the guarantees

appropriate, under Article 46, with respect to this transfer.

3. The controller provides a copy of the personal data subject to

of a treatment. The controller may require the payment of reasonable fees based on

administrative costs for any additional copies requested by the data subject.

When the data subject submits his request electronically, the information is

provided in a commonly used electronic form, unless the data subject

request otherwise.

4. The right to obtain a copy referred to in paragraph 3 does not affect the rights and freedoms

from others. »

137. The plaintiff argues that the defendant did not facilitate the exercise of her rights, and what

showed reluctance in the face of his requests for explanations (for example by not transmitting

the information required under Article 14). The defendant responds that the complainant did not

Decision on the merits 56/2021- 28/39

did not ask for this information to be sent to him. This question having been discussed more

above and the defendant's argument having been dismissed, the Litigation Chamber refers to point

II.3.

138. The complainant also asserts that “Considering that (the complainant) did not exercise her right of access while

that she explicitly asked for justifications on the consultations comes under a certain

bad faith” (conclusions of the complainant p.18).

139. According to the constant position of the Litigation Chamber34, the formulation of a request for access

or the exercise of any other right – even if it was incomplete or based on an erroneous provision

or in support of a misunderstanding or interpretation of the right invoked – cannot be used as

pretext for the data controller not to give a useful follow-up. This needs to be looked at

case by case.

140. In the present case, on reading the emails exchanged between the parties, the Litigation Division

is of the opinion that it is not sufficiently apparent that the complainant requested the exercise of her right

access. In her emails, the complainant mainly requests explanations of the

procedures for access to CCP data, and on the sanctions against an employee abusing

her access to the file, including her ex-husband35.

141. Nevertheless, although a distinction should be made between emails requesting explanations as to

procedures for access to CCP data as well as on the sanctions against an abusive employee

of his access to the file of a request for access to his personal data, the Chamber

Litigation recalls that the SPL formally requested the defendant (on behalf of

complainant), in her letter of October 21 (exhibit 4 from the complainant), to send the

complainant the information under Article 14 and to follow up on his right of access to the data

held by the defendant. The defendant did not respond to this letter.

34 See in particular the decision of the Litigation Chamber 41/2020 of July 29, 2020

35 We can thus read in the complainant's emails to the defendant's DPO, for example:

-"(…) Thank you for having taken into consideration the seriousness of the facts. However, I do not desire outright dismissal

of my ex-husband, I would just like the sanction taken against him to make him aware that by his

behavior it brought me financial harm…" (email of April 08, 2019)

- "However, I would like to know what an employee incurs if he breaches data protection compliance" (email

March 13, 2019)

- "Anyway, before making my complaint effective, I would like to know what my ex-husband incurs for having

committed this intrusion into my private life. Then I will mention his name, which will only allow you to

sanction" (email of April 5, 2019)

142. The defendant therefore violated Article 15 GDPR by not responding to the access request of

Decision on the merits 56/2021- 29/39

the complainant.

II.5- Regarding the independence of the Data Protection Officer

143. The Complainant argues that the Respondent's Data Protection Officer (DPO) does not

does not fulfill the condition of independence arising from Article 38.3 GDPR, due to its

previous professional career, the combination of his DPO functions with those of CISO (Chief

Information Security Officer), and because she allegedly "represented the interests" of the

defendant during his interactions with the complainant. These arguments are examined

successively below.

II.5.1-The professional career of the DPO does not lead to a conflict of interest

144. The complainant maintains that the DPO was previously the director of the legal department of the defendant. However, the defendant explains that the DPO indeed occupied this function, but at the within the "W" company, having no connection with it. This argument is therefore rejected.

II.5.2-The combination of DPO and CISO functions does not lead to a conflict of interest

145. Article 38.6 GDPR states that “The Data Protection Officer may perform other assignments and tasks. The controller or processor shall ensure that these assignments and tasks do not involve a conflict of interest”.

146. The EDPB guidelines teach that the DPO “cannot practice within the organization a function that leads it to determine the purposes and means of data processing to personal character. Due to the specific organizational structure of each organization, this aspect must be studied on a case-by-case basis. »36

147. This is therefore a substantial conflict of interest, which may arise in particular when the same person is likely to act both in the position of controller and controlled (e.g. a project manager or department involving data processing, who would perform the the function of DPO when he would be called upon in this capacity to control the compliance of the treatment as part of his project).

36 EDPB, Guidelines for Data Protection Officers (DPOs), 5 April 2017, p19

148. In particular, this involves taking into account the decision-making power or not that the delegate has protection of data in the exercise of his other function37.

149. The complainant raises a conflict of interest in the combination of the functions of DPO and CISO by a same person within the defendant because the latter would exercise decision-making power the technical and organizational measures put in place within the SA, measures that the complainant considers insufficient and contrary to Article 32 GDPR.

150. The defendant explains in its pleadings as well as during the hearing that the functions of DPO and CISO are not executive functions, but advisory functions,

risk identification. During the hearing, the defendant's DPO explained that it presents,

management of the company, the risks and their importance and that it is up to this management

to decide whether the measures put in place are sufficient to remedy the risks. She has by

further specified that in the event of disagreement between it and the management concerning the measures taken

and notwithstanding the remarks addressed to the latter, the decision is not within his competence. She

further clarifies that security measures are the responsibility of the IT department, and not of

that of the CISO.

151. It also indicates that in the organization chart of the defendant SA, the functions of CISO and DPO

arise from the “second line of defence”, the first being made up of the functions

operational, unlike the second.

152. Insofar as the CISO is not, in the present case, responsible for a department

operational38, the complainant cannot be followed when she claims that the person being both

DPO and CISO exercises decision-making power regarding technical and organizational measures

implemented within the defendant.

II.5.3-The content of the DPO's responses to the complainant does not indicate a violation of its role

153. Article 38.4 GDPR states that “Data subjects may contact the

data protection officer on all matters relating to the processing of

their personal data and the exercise of the rights conferred on them by this

regulation”.

154. The DPO therefore acts, among other things, as a contact point for people who wish to

exercise their rights with the data controller.

37 Rosier, K., “Data protection officer: a multifaceted function” in The general regulation on the

data protection (RGPD/GDPR), Brussels, Éditions Larcier, 2018, p.578

38 Conversely, the Litigation Chamber considered that there is a conflict of interest in the case where a DPO is both

responsible for several operational departments (see decision 18/2020 p15 s)

155. The complainant argued that the DPO would have taken up the cause of the defendant (her employer),

instead of investigating the complaint made by the complainant independently. In doing so, the

complainant relies on the content of the responses formulated by the DPO to the complainant's emails,

from which it appears that it uses the terms “we” (“we cannot give you more

information", "we have apologized", "we have of course taken the

coercive measures” …).

156. However, although the complainant expressed her frustration with the quality of the support

the DPO for the facilitation of its rights, it does not emerge from the analysis of the written exchanges between the

complainant and the DPO that the latter would not have behaved in accordance with its role. Like

the DPO indicated during the hearing, the complainant's requests focused mainly on the

sanction incurred by her ex-husband, which does not come under the personal data of the

complainant. The Litigation Chamber also recalls that the DPO is bound by the duty to

confidentiality (article 38.5), and follows it when she explains at the hearing that she could not

this reason not respond to the complainant regarding the sanctions incurred by her ex-husband.

157. In conclusion, the complainant cannot be followed when she claims that the DPO does not fulfill the

condition of independence due to his previous professional career, the accumulation of his

functions of DPO with those of CISO, and because of the fact that she would have "represented the interests

of the defendant during his interactions with the complainant.

158. There is therefore no violation of Article 38 GDPR.

4.

Regarding corrective measures and sanctions

4.1- Corrective measures and sanctions

Under the terms of Article 100 LCA, the Litigation Chamber has the power to:

1° dismiss the complaint without follow-up;

2° order the dismissal;

3° order a suspension of the pronouncement;

4° to propose a transaction;

5° issue warnings or reprimands;

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

Decision on the merits 56/2021- 32/39

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

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

9° order the processing to be brought into conformity;

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

data recipients;

11° order the withdrawal of accreditation from certification bodies;

12° to issue periodic penalty payments;

13° to impose administrative fines;

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

international;

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

data on file;

16° decide on a case-by-case basis to publish its decisions on the website of the Authority for the protection of

data.

159. The aforementioned Article 100 specifies the list of sanctions in Article 58.2 of the GDPR.

As for the administrative fine which may be imposed pursuant to Article 83 of the GDPR and the

articles 100, 13° and 101 LCA, article 83 of the GDPR provides:

“1. Each supervisory authority shall ensure that the administrative fines imposed under the

this Article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are, in

each case, effective, proportionate and dissuasive.

2. Depending on the specific characteristics of each case, the administrative fines are imposed in

in addition to or instead of the measures referred to in points (a) to (h) and (j) of Article 58(2). For

decide whether to impose an administrative fine and to decide the amount of the fine

administrative procedure, due account shall be taken, in each case, of the following elements:

(a) the nature, gravity and duration of the breach, taking into account the nature, scope or

purpose of the processing concerned, as well as the number of data subjects affected and the level

damage they have suffered;

b) whether the breach was committed willfully or negligently;

c) any action taken by the controller or processor to mitigate the damage

suffered by the persons concerned;

Decision on the merits 56/2021- 33/39

d) the degree of responsibility of the controller or processor, taking into account the

technical and organizational measures they have implemented pursuant to Articles 25 and 32;

e) any relevant breach previously committed by the controller or sub-processor

treating;

(f) the degree of cooperation established with the supervisory authority with a view to remedying the breach and

mitigate any negative effects;

(g) the categories of personal data affected by the breach;

h) how the supervisory authority became aware of the breach, including whether and in

the extent to which the controller or processor notified the breach;

(i) where measures referred to in Article 58(2) have previously been ordered to

against the controller or processor concerned for the same purpose, compliance

of these measures;

(j) the application of codes of conduct approved under Article 40 or mechanisms for

certification approved under section 42; and

k) any other aggravating or mitigating circumstance applicable to the circumstances of the case, such as

that the financial benefits obtained or losses avoided, directly or indirectly, as a result of

the violation ".

160. It is important to contextualize the breach of Articles 32, combined with Articles 5 and 24, and 15□

GDPR to identify the most appropriate corrective measures.□

161. In this context, the Litigation Chamber will take into account all the circumstances of□

the case, including - within the limits that it specifies below - the reaction communicated□

by the defendant to the amount of the envisaged fine which was communicated to it (see retroacts of□

the procedure). In this respect, the Litigation Division specifies that the said form mentions□

expressly that it does not imply a reopening of the debates. It pursues the sole purpose of□

collect the reaction of the defendant on the amount of the proposed fine.□

162. The Litigation Chamber also wishes to specify that it is sovereignly incumbent upon it□

quality of independent administrative authority - in compliance with the relevant articles of the GDPR□

and the ACL - to determine the appropriate corrective action(s) and sanction(s).□

163. Thus, it is not for the plaintiff to ask the Litigation Chamber to order□

such or such corrective measure or sanction. If, notwithstanding the foregoing, the Complainant□

nevertheless had to ask the Litigation Chamber to pronounce one or the other measure□

and/or sanction, it is therefore not for the latter to justify why it would not retain□

not one or the other request made by the complainant. These considerations leave intact□

Decision on the merits 56/2021- 34/39□

the obligation for the Litigation Chamber to justify the choice of measures and sanctions to which□

it judges, (among the list of measures and sanctions made available to it by articles 58 of the□

GDPR and 100 of the ACL) appropriate to condemn the party in question.□

164. In the present case, the Litigation Chamber notes that the plaintiff requests, in particular, from the Chamber□

Litigation that it orders compliance with the GDPR (in particular with Article 32, combined□

in articles 5 and 24) of the consultations of the executives' CCP.□

165. The complainant also requests the imposition of an administrative fine. The Litigation Chamber□

emphasizes that it is responsible for ensuring the effective application of the rules of the GDPR. other measures,□

such as the order for compliance or the prohibition to continue certain processing by□

example, allow them to put an end to a breach observed. As it appears

of recital 148 of the GDPR, sanctions, including administrative fines, are imposed

in the event of serious violations, in addition to or instead of the appropriate measures which

are required. Therefore, the administrative fine can certainly come to sanction a breach

serious which would have been remedied during the proceedings or which is about to be. It does not

remains that the Litigation Chamber will take into account the measures taken following

the incident in setting the amount of the fine.

4.2- As to breaches

166. The Litigation Chamber found a breach of Article 32, combined with Articles 5 and 24,

as well as Article 15 GDPR.

167. The Litigation Division also takes note of the fact that the defendant has since its

conclusions and during the hearing, recognized that a breach of section 32 may be alleged against him39.

She also explained a new organizational measure introduced following the incident (only

two executives now have access to the NBB's CCP register, and they now have them

a register which will be compared with that held by the NBB as a control measure).

168. Although it takes note of these efforts, the Litigation Division is of the opinion that they are not

sufficient and that other measures must be taken by the defendant to put itself in

compliance with its obligations under the GDPR. Therefore, the Litigation Chamber imposes on him

an order for compliance of the process of access by executives to the CCP. She recommends

moreover strongly the keeping of a log register of accesses, to be compared with that kept by the

BNB, and in compliance with all the indications mentioned above (see above II.2.2).

39 Additional conclusions and summary of Y p.9

169. The Litigation Division also considers that the sensitive nature of the data processed on a large

scale by the defendant should have led it to reinforce its compliance with the principles

of the GDPR (including the security of processing) well before, in particular by anticipation

risks associated with such breaches.

170. In addition to this compliance order, the Litigation Division is of the opinion that, in addition,

an administrative fine is justified in this case for the following reasons, reasons analyzed on

basis of article 83.2 GDPR and in accordance with the recent teaching of the Court of Markets.40

171. The rights of data subjects, as well as the principle of security, are part of the essence

of the GDPR and their violation are punished with the highest fines, in accordance with Article 83.5

GDPR. In this spirit, these serious breaches can be sanctioned with fines

proportionately high, depending on the circumstances of the case. In this regard, one can

cite the Group 29 Guidelines on the application and setting of fines

administrative41, according to which:

“Fines are an important instrument that supervisory authorities should use in

the appropriate circumstances. Supervisors are encouraged to take an approach

carefully considered and balanced when applying corrective measures to respond to

violation in a way that is both effective and dissuasive and proportionate. It's not about

regard fines as a last resort or fear imposing them, but, on the other hand,

nor should they be used in such a way that their effectiveness would be impaired.

diminished. »

172. In paragraph (a), section 83.2. concerns “the nature, gravity and duration of the breach,

taking into account the nature, scope or purpose of the processing concerned, as well as the

number of data subjects affected and the level of harm they suffered”.

173. In the present case, the Litigation Chamber notes that both the principle of security (article

5.1, f) GDPR) (and the obligations arising therefrom – Article 32 of the GDPR) that the right of access (Article

15), are essential principles of the protection regime put in place by the GDPR. The principle

responsibility set out in Article 5.2. of the GDPR and developed in Article 24 is also at the

heart of the GDPR and reflects the paradigm shift brought about by it, i.e. a shift

a regime that relied on prior declarations and authorizations from the supervisory authority

towards greater accountability and responsibility of the data controller. The respect

40 Brussels Court of Appeal, 19th chamber, market court section, judgment of 27 January 2021, p21-24

41 Group 29, Guidelines on the application and setting of administrative fines

for the purposes of Regulation (EU) 2016/679, WP 253, adopted 3 October 2017, p7

of its obligations by the latter and its ability to demonstrate it are therefore only more

important. Breaches of these principles constitute serious breaches.

174. With regard more specifically to the nature of the data accessed improperly, the Chamber

emphasizes that the defendant is active in the banking sector and deals with large volumes

sensitive financial data (data relating to the credits of the persons concerned).

In this case, the data relating to the complainant's credits were improperly consulted on

a period extending from April 2016 to August 2018, and this on no less than 20 occasions. Bedroom

concludes that the abusive consultations in question, both by their nature and their seriousness and

their duration constitute serious offences.

175. She also notes that in the absence of a complaint lodged by the complainant, it is not unreasonable

to think that such abusive consultations could have continued and gone unpunished, since

it was following the complaint that the defendant took additional measures and sanctioned his

offending employee.

176. Furthermore, the Litigation Chamber notes that the personal data of nearly 6 million

of persons appear in the CCP register of the BNB, and that the employees of the defendant,

including executives, consult them on a regular basis.

177. As to the question of whether the breaches were committed deliberately or not (for

negligence) (art. 83.2.b) of the GDPR), the Litigation Chamber recalls that "not deliberately"

means that there was no intent to commit the violation, although the person responsible for the

processing has not complied with the duty of care incumbent upon it under the law. In

In this case, the Litigation Chamber is of the opinion that the breaches noted - however serious

- do not reflect a deliberate intention to violate the GDPR on the part of the defendant.

Paragraph d) of Article 83.2 GDPR then returns to the degree of responsibility of the person responsible for the processing, taking into account technical and organizational measures (Art. 32 GDPR). The Chamber refers here to the developments above, from which it appears that the defendant had not put no security measures in place regarding executive access to data in the CCP register before abusive consultations. It is also apparent from the statements of the defendant's DPO that following this incident, the only new measure put in place for this purpose remains limited (reduction the number of executives having access to the CCP register from five to two and kept by these executives from one access register).

178. Finally, Article 83.2(e) concerns “any relevant violation previously committed by the controller or processor”. The Litigation Chamber notes in this regard that the group to which the defendant belongs was sanctioned by another supervisory authority.

Decision on the merits 56/2021- 37/39

179. The Chamber notes the Respondent’s efforts regarding its collaborating employees (new GDPR training, staff awareness, etc.) but notes, as indicated above, that the additional security measures specific to executive access remain weak. The only new measure following the incident consists in fact of a reduction from 5 to 2 executives access the PCB. The Chamber also notes that the Respondent only realized in December 2020 the possibility of comparing the access list of the executives it maintains (henceforth) with that held by the BNB, while the complainant notified the consultations abusive and that they were recognized by their author (the complainant's ex-husband) in 2019.

180. The Litigation Chamber notes that the other criteria of Article 83.2. of the GDPR are neither relevant or likely to influence its decision on the imposition of a fine administrative and its amount. Pursuant to Article 83.5 a) GDPR, breaches of all these provisions can amount to up to 20,000,000 euros or in the case of a company, up to 4% of the total worldwide annual turnover of the previous financial year. The maximum amounts

fines that may be applied in the event of a violation of these provisions are higher than those
provided for other types of breaches listed in Article 83.4. of the GDPR. Is about
breaches of a fundamental right, enshrined in Article 8 of the Charter of Fundamental Rights
of the European Union, the assessment of their seriousness will be made, as the Litigation Chamber has
already had the opportunity to point this out, in support of Article 83.2.a) of the GDPR, independently42.
181. The Litigation Chamber recalls the provisions of Article 83.4 GDPR, which lists the
infringements for which the fine may amount to EUR 10,000,000 or, in the case of
company, up to 2% of the total worldwide annual turnover of the preceding financial year, the
the higher amount of the two being applicable. Breaches of articles 8, 11, 25 to 39,
42 and 43 are retained. Such offenses therefore cover, inter alia, a breach of
the obligation to introduce appropriate technical and organizational measures to ensure the
compliance with the GDPR, a breach of the obligation to secure processing, the obligation to
data protection by design and data protection by default, or
the obligation to keep processing records. In the present case, as indicated above, the Chamber
Litigation notes both a breach of the obligation to introduce technical and
appropriate organizational measures to ensure compliance with the GDPR, as well as with the security obligation
processing, as well as the obligation to protect data from the design and protection
default data. The maximum amount of the fine in the specific case, as provided
by Article 83.5 is therefore EUR 10,000,000.
42 See.
https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-64-2020.pdf
the Litigation Chamber
64/2020
decision
(point
54),

of

the

available

on

182. The defendant is also part of a large multinational, which it confirmed during the

the hearing. In determining the amount of the fine, the Litigation Division takes into account

of the notion of business (article 83. 5 of the GDPR). The Litigation Chamber also holds

account of the opinion of the European Data Protection Board, of which it retains all

particularly the following:

“In order to impose effective, proportionate and dissuasive fines, the supervisory authorities

will refer to the definition of the concept of undertaking provided by the CJEU for the purposes of the application of

Articles 101 and 102 TFEU, namely that the concept of undertaking must be understood as a unit

economic activity that can be formed by the parent company and all the subsidiaries concerned. In accordance

Union law and case-law, an enterprise should be understood to mean the economic unit

engaged in commercial or economic activities, regardless of the legal person

involved (recital 150). »

183. In conclusion, in view of the elements developed above specific to this case, the Chamber

Litigation considers that the aforementioned breaches justify that as a sanction

effective, proportionate and dissuasive as provided for in Article 83 of the GDPR and taking into account the

assessment factors listed in Article 83.2 GDPR and the defendant's reaction to the

proposed fine form, a compliance order with a fine

administrative proceedings in the amount of 100,000 euros (article 100.1, 13° and 101 LCA) be pronounced

against the defendant.

184. The amount of 100,000 euros remains in view of these elements proportionate to the breaches

denounced. This amount also remains well below the maximum amount provided for by

Article 83.5 GDPR, of 10,000,000 euros (see above).

185. This amount is justified for the reasons set out above, including the sensitive nature of the data

subject to the disputed processing (financial data relating to the complainant's credit),

the extended period during which the processing took place, or the number of times

at which these treatments took place (20). Other considerations justifying this amount

rely on the fact that few additional measures have been put in place since the incident by

the defendant to reinforce the safety of its treatments, on the fact that without the introduction of

the complaint, it is not unreasonable to think that the abusive consultations could have continued

without the defendant's attention being drawn to the flaws in its security measures,

which also processes a large volume of sensitive financial data (6 million

consultations in the CCP register per year, according to his declarations). The Litigation Chamber is of the opinion

that a lower amount of fine would not meet, in this case, the criteria required by Article

83.1. of the GDPR according to which the administrative fine must not only be proportionate,

but also effective and dissuasive. These elements constitute a specification of the obligation

Decision on the merits 56/2021- 39/39

of Member States under European Union law, based on the principle of

loyal cooperation (Article 4.3 of the Treaty on European Union).

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

Litigation and in accordance with Article 100.1, 16° of the LCA, this decision is published

on the website of the Data Protection Authority by deleting the data

identification of the parties, since these are neither necessary nor relevant in the context of

publication of this decision.

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

access to the NBB's CCP register by executive employees in accordance with Articles 5.1.f

and 32 GDPR. To this end, the Litigation Division grants the defendant a period of

three months and expects her to submit a report to him within the same period concerning the

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 100,000 euros for violation of articles

aforementioned

Under Article 108.1 LCA, this decision may be appealed to the Court of

contracts (Brussels Court of Appeal) within 30 days of its notification, with

the Data Protection Authority as defendant.

(Sé) Hielke Hijmans

President of the Litigation Chamber