Litigation Chamber

Decision on the merits 127/2022 of 19 August 2022

File number: DOS-2019-05244

Subject: Complaint against a medical analysis laboratory for violation of the principles

of integrity and confidentiality and transparency

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

Hijmans, chairman, and Messrs. Christophe Boeraeve and Frank De Smet, members;

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

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

to 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

ACL);

Having regard to the internal regulations as approved by the House of Representatives on 20

December 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 :

X, hereinafter "the plaintiff"

The defendant: Medical Analysis Laboratory, represented by Sébastien Popijn, hereinafter:

"the defendant"

I. Facts and procedure

Decision on the merits 127/2022 - 2/16

1. On October 4, 2019, the complainant filed a complaint with the Protection Authority

data against the defendant.

2. The complainant suspects

the

medical analysis laboratory (hereinafter: Laboratory

medical analyses) for not having carried out an impact analysis relating to the protection of

data, of not informing people correctly and of dealing with categories

specific data, in this case data concerning health, via a site

unsecured internet.

The complainant states that he had dealings with the analysis laboratory on several occasions

medical within the framework of medical analyses. He has been informed that his doctor has access to

results of its analyzes electronically. However, he realizes that the site of the Laboratory

of medical analyzes includes a page for accessing medical analysis data

entitled "Cyberlab" in an unsecured http protocol.

3. On October 29, 2019, the complaint was declared admissible by the Front Line Service on

the basis of articles 58 and 60 of the LCA and the complaint is transmitted to the Litigation Chamber

under article 62, § 1 of the LCA.

4. On November 27, 2019, the Litigation Chamber decides to request an investigation from the

Inspection Service, pursuant to articles 63, 2° and 94, 1° of the LCA.

5. On November 29, 2019, in accordance with Article 96, § 1 of the LCA, the Chamber's request

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

as the complaint and the inventory of parts.

6. On 8 September 2021, the investigation by the Inspection Service is closed, the report is attached to the

file and this is transmitted by the Inspector General to the President of the Chamber

Litigation (art. 91, § 1 and § 2 of the LCA).

The report contains findings relating to the subject of the complaint and carries out the

following findings:

1. The defendant can be considered as the controller

2. Insufficient security of health data in violation of Articles 5.1.f), 24, 25

and 32 GDPR.

3. Absence of impact analysis relating to the protection of data in violation of the

articles 35.1 and 35.3 of the GDPR).

4. Lack of information regarding the processing of data in violation of the

articles 12 to 14 of the GDPR.

Decision on the merits 127/2022 - 3/16

7. On September 21, 2021, the Litigation Chamber decides, pursuant to Article 95, § 1, 1° and

of article 98 of the LCA, that the case can be dealt with on the merits.

8. On September 21, 2021, the parties concerned are informed by registered letter of the

provisions as set out in article 95, § 2 as well as in article 98 of the LCA. They are

also informed, pursuant to Article 99 of the LCA, of the deadlines for transmitting their

conclusions.

The deadline for receipt of the defendant's submissions in response has been set

on November 2, 2021, that for the plaintiff's reply submissions on November 23

2021 and finally that for the conclusions in reply of the defendant on December 14

2021.

9. On September 27, 2021, the defendant requested a copy of the file (art. 95, §2, 3° LCA),

which is transmitted to him on October 6, 2021.

10. On November 2, 2021, the Litigation Chamber receives the submissions in response from the

defendant.

11. On November 7, 2021, the Litigation Chamber receives the submissions in reply of the

complainant.

12. On December 9, 2021, the Litigation Chamber receives the submissions in reply from

of the defendant.

13. On July 25, 2022, the Litigation Chamber informed the defendant of its intention

to proceed with the imposition of an administrative fine as well as the amount thereof, in order
to give the defendant the opportunity to defend himself before the sanction is
actually inflicted.

14. On August 15, 2022, the Litigation Chamber receives the defendant's reaction
concerning the intention to impose an administrative fine and the amount thereof.

II. Motivation

II.1. Responsibility for processing

15. In its investigation report, the Inspection Service (hereafter: SI) determines that the party
defendant may be qualified as a data controller. This position is
initially contested by the defendant, but finally accepted in its
summary conclusions, following the complainant's reply conclusions.

16. The Litigation Chamber decides that the defendant can be qualified as
responsible for processing given that it determines the purposes and means of the
treatment.

17. It nevertheless recalls that under the principle of responsibility of Article 24 of the GDPR,
the defendant must itself be able to establish its responsibilities and its
obligations under the GDPR. The Litigation Chamber further adds that the
changes in the position of the defendant during the procedure bring
obvious confusion in its defence, since originally it advances for example that it
is not subject to the obligation to carry out a DPIA because it is only a subcontractor1
(and that the subcontractors have no obligation to carry out the DPIA) to then indicate that
the absence of carrying out a DPIA is due to the fact that, originally, the processing
did not meet the criteria for making one. 2 These positions are good
obviously incompatible with each other.

II.2. Complainant's interest.

18. It appears from the file that the plaintiff's doctor had the defendant carry out

several medical analyzes for his patient. The defendant therefore deals or has dealt with

personal data of the complainant. He therefore has an interest in acting.

in this file.

II.3. Finding 1: insufficient security of health data (articles 5.1.f), 24, 25

and 32 GDPR)

19. It appears from the investigation report that the defendant has a website. The home page

of this website informs another page of the medical analysis laboratory under a

entitled "Consult the results", which refers to the "Cyberlab", the results server in

the defendant's line which allows doctors to access the results and

test histories of their patients.

20. The IS was able to observe during its first technological investigation report of January 14, 2021

(hereafter: the first technological report) that this website does not contain

encryption (the username and password collected are transmitted unencrypted), being

given that it uses an “http” protocol instead of an encrypted “https” protocol.

1 Defendant's submissions, p. 9.

2 Defendant's Summary Conclusion, p. 7.

21. The IS notes on this occasion that “The Cyberlab access site is therefore unsecured and

is susceptible to "man in the middle" attacks. The identifier and the

password collected are transmitted unencrypted […]”.

22. Following the responses provided by the Respondent during the investigation, a follow-up report

of the technological investigation report is produced on July 6, 2021 (hereinafter, the report of

followed). This report establishes in particular that since the establishment of the first report

technological, the “Cyberlab” “has been secured since it is accessible by means of the protocol

https instead of the http protocol. The use of this secure protocol prevents the

disclosure of connection information and therefore access to the results of analyzes of

patients with "Man in the Middle" attacks. »

23. The second report adds that “the encryption protocol is TLS 1.2 for which several

vulnerabilities exist” and that “compared to the initial report, we can notice

progress [with regard to] securing information in transit since

the implementation of the TLS 1.2 protocol has been made instead of a simple connection

http. ".

24. Based on these two technological reports, the IS finds a violation of Articles

5.1.f), 24, 25 and 32 of the GDPR.

25. The defendant's arguments are summarized as follows:

- the grievance against him is no longer relevant, as noted by the IS and

acknowledged by the complainant in his conclusions;

- before the implementation of encryption, the site was not devoid of security measures

security, since the doctor wishing to access it must have an identifier and a

personal secret code;

- a "Man in the Middle" type attack assumes that the hacker has previously taken

control of the physician's IT infrastructure. In which case he would have no

access only to the results of a patient's analysis;

- No attack of this type has been detected and the software publisher Cyberlab does not seem

not require the installation of an https certificate;

- the wording "guarantee appropriate security" of article 5.1.f) of the GDPR "assumes

to look at the existing environment and not to reason in abstracto;

- the defendant took the decision to strengthen the security of access to the data by

setting up a system of “double identification of doctors”3, which will require

their prior consultation.

3 Terminology used by the defendant.

26. Based on the investigation report and the arguments of the parties, the Litigation Chamber finds that the defendant's Cyberlab website was not secure at the time of the complaint and the initiation of the investigation. Following the IS's contact with the defendant, the site was secured via the implementation of the TLS 1.2 protocol, on a date indefinite period located between the first technological report of January 14, 2021 and the second July 6, 2021 technology report.

27. Beyond the considerations and arguments raised by the defendant, the protocol TLS is a basic encryption protocol that has been around since 1999. Any entity that aims to ensure standard security of data passing through its website in fact or should in fact make use of. This is a standard that is very widely recommended4.

28. This is all the more valid for a platform that processes and provides access to results of medical analyzes of hundreds or thousands of patients5. This standard – and more specifically its TLS 1.2 version - was only implemented after the IS took contact with the defendant.

29. The principle of integrity and confidentiality, set out in Article 5.1.f) of the GDPR is drafted as following :

“Personal data must be processed in such a way as to guarantee the security appropriate treatment of personal data, including protection against the processing unauthorized or unlawful and against accidental loss, destruction or damage, at using appropriate technical or organizational measures (integrity and privacy) "

It is further developed in Article 32 of the GDPR.

30. In this case, the Litigation Chamber decides that a web page allowing doctors to

remotely consult the results of medical analyzes of patients without offering

encryption, violates the principle of integrity and confidentiality enshrined in Articles 5.1.f) to

GDPR Article 32.

31. Beyond these articles, the SI also considers that as an analytical laboratory

medical data, the defendant processes health data on a daily basis. He was from his

responsibility for implementing technical and organizational measures

appropriate and ensure data protection by design and by default,

in accordance with Articles 24 and 25 of the GDPR and therefore concludes that these articles have been violated.

4 See for example the recommendations of the CNIL on the security of websites; EDPS guidelines

concerning the protection of personal data processed by web services provided by EU institutions (point 82).

5 The defendant stating in its conclusions that it was processing 50 analyzes per day before the start of the pandemic

of COVID and that this figure has greatly increased since then.

32. The defendant defends itself on finding number 1 as a whole with the

arguments summarized in point 25 and does not distinguish between violation of Articles

5.1.f) and 32 on the one hand and articles 24 and 25 on the other hand.

33. The Litigation Chamber considers that the finding of violation of Articles 5.1.f) and 32 of the

GDPR is sufficient to penalize the breach relating to the security of the processing.

34. Furthermore, in these summary submissions, the defendant states “that with a view to

to further strengthen security of access to data, the medical analysis laboratory has

taken the decision to set up a system of double identification of doctors". The

Litigation Chamber understands from this sentence that the defendant refers to

a multi-factor authentication system. In this case, the Litigation Chamber

stresses the importance of setting up a strong authentication system, which could

be bifactorial. She adds, although this aspect is not part of the findings of the

IF, that the absence of a strong authentication system could raise questions as to the

compliance with the principle of confidentiality and integrity provided for in Articles 5.1.f) and 32 of the GDPR.

II.4. Finding 2: Absence of impact analysis relating to data protection

(Articles 35.1 and 35.3 of the GDPR).

35. For the Inspection Service, the defendant violated Articles 35.1 and 35.3 of the GDPR by not

not carrying out a Data Protection Impact Assessment, although it deals with a large

health data scale.

36. The defendant disputes the fact that at the time it was processing large-scale data

scale, indicating that it only processed about fifty analyzes per day. She believes that

the notion of “large scale” included in Article 35.3.b) is not sufficiently objective. She

is also based on information on the CNIL website which indicates

that medical analysis laboratories must check, depending on their project, whether it is

necessary to carry out a data protection impact analysis, which for the

defendant indicates that this obligation is not systematic6.

37. She adds that the number of analyzes processed by the medical analysis laboratory has

significantly increased due to the Covid-19 pandemic. Therefore, she

believes today that it is entering into the conditions for the processing of large-scale health data

scale and therefore commissioned a DPIA

38. The complainant, for his part, considers that the processing operations are indeed data processing operations

health care operated on a large scale. He considers that these fall under point 5 of

6 https://www.cnil.fr/fr/cnil-direct/question/laboratoire-danalyse-de-biologie-medicale-que-faire

Decision of the General Secretariat for ODA No. 01/2019 of 16 January 20197 which is formulated

as following :

"When special categories of personal data within the meaning of Article

9 of the GDPR […] are systematically exchanged between several managers of the

treatment. ".

39. The complainant also considers that even if the processing operations do not fall under this point, they still constitute processing of health data carried out on a large scale. ladder. The Complainant disputes that the definition of large scale is left entirely at the discretion of the supervisory authority, since it is marked out by recital 91 of the GDPR and the Article 29 Working Party (G29) Guidelines on Data Protection Officers data protection8.

40. The question brought before the Litigation Division is whether the defendant was subject to the obligation to carry out a DPIA on the basis of Articles 35.1 and 35.3 of the GDPR before the complaint is lodged, due to the fact that the processing of data it performs constitute large-scale data processing.

41. The Litigation Chamber first notes that it is undisputed that the Defendant processes health data within the meaning of Article 9.1 of the GDPR. The House Review litigation therefore focuses on the notion of "large scale".

42. The Litigation Chamber notes that the defendant criticizes the notion of "large scale" calling it imprecise.

43. The Litigation Chamber agrees that the notion of “large scale” is subject to assessment, but it denies that this is a source of legal uncertainty. In effect, both the GDPR9, and national and European recommendations make it possible to clarify the criteria that trigger an obligation to carry out a DPIA. These are included in the Data Protection Impact Assessment Guide published by ODA on its website10 and which contains four criteria taken from the guidelines to determine whether processing is carried out on a large scale11. He these are the following criteria:

-

the number of people concerned, either in absolute value or in proportion to the population considered;

7 Available at: https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf

8 Available at: https://ec.europa.eu/newsroom/article29/items/612048

9 GDPR, recital 91.

10 Data Protection Authority, “Guide to Data Protection Impact Assessment”, version 4.0 of 21 April

2021, p. 2-7. (Available at: https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-

data-protection.pdf)

11 Ibid., p. 6.

the volume of data and/or range of different data elements processed;

the duration or permanence of the data processing activity;

the geographic scope of the processing activity.

-

-

-

44. The Litigation Chamber also points out to the Respondent that it contributes

itself to maintain a certain subjectivity of this notion by referring in its

conclusions to vague elements by considering "only originally" its activities

did not constitute a large-scale processing, but that "the analyzes processed by the

medical analysis laboratory having considerably increased due to the

Covid-19 pandemic”, she believes that she is now carrying out large-scale treatments

ladder. The defendant should have, on the basis of the liability principle of Article 24,

clarify its interpretation of the notion of “large scale” by indicating the criteria

objectives on which it bases itself to estimate that its activities have finally entered into the

category of large-scale treatments, whereas according to her, they did not fulfill

this criterion at the outset.

45. In the present case, several factors allow the Litigation Division to conclude that the

defendant was indeed subject to a DPIA before it decided to carry it out.

46. First of all, the Litigation Chamber does not have any information indicating that

the extent of the data processing carried out by

the defendant would have

radically evolved due to the COVID-19 pandemic to become a treatment at

large scale. The defendant indeed argues that before the COVID-19 pandemic, the

laboratory carried out about fifty analyzes per day, without specifying the number

analyzes carried out currently or during the pandemic.

47. In addition, the DPIA document produced by an external service provider12 advances the

following conclusion: “The data processing described must be considered as

likely to cause a high risk to the rights and freedoms of individuals

physical. Indeed, the analysis of the samples as well as the rendering of the results of the analyzes

process special categories of personal data on a large scale.

A DPIA must be carried out by the medical analysis laboratory. »

48. The Litigation Chamber therefore concludes that the processing at the time of the complaint and the

investigation report are large-scale processing.

12 Document provided to the Litigation Division on the proposal of the defendant following the exchange of conclusions.

This document had not yet been drawn up during the investigation by the Inspection Service.

49. Surprisingly, the Litigation Division is of the opinion that the processing operations in question

fall under the definition of point 5 of the Decision of the General Secretariat n°01/2019 of 16

January 2019 which is worded as follows:

"When special categories of personal data within the meaning of Article

9 of the GDPR […] are systematically exchanged between several managers of the

treatment. ".

It is in fact established that the defendant carries out analyzes for numerous

physicians, themselves considered to be responsible for the processing, who may by

read the results of the analyses. For the Litigation Chamber, the realization

of a DPIA could therefore also have been mandatory on this basis.

Finally, the Litigation Chamber recalls that under Article 35.1 of the GDPR, an analysis

must be carried out before the envisaged treatment is carried out13.

50. Based on the above elements, the Litigation Chamber concludes that the defendant

should have already carried out a DPIA before the complaint was lodged, and that by not

not having done so, the defendant violated Articles 35.1 and 35.3 of the GDPR.

II.5. Observation 3: lack of information concerning the processing of data (articles

12 to 14 GDPR)

51. It appears from the technological investigation report of January 14, 2021 that no life policy

information was available on the medical analysis laboratory website on that date.

52. According to its legal adviser, the medical analysis laboratory would have planned a posting

GDPR information in its own collection centers. That being the case, he recognizes

that this represents only a small part of the patients for whom the laboratory

of medical analyzes is responsible for carrying out analyses.

53. The report of July 6, 2021 follow-up to the technological investigation report showed that a

privacy policy was now on the medical analysis laboratory website.

54. The Inspection Service finds a violation of the obligation to provide information

provided for in Articles 12 to 14 of the GDPR given that no privacy policy was

present on the website at the time of the first technological report.

55. Firstly, the defendant disputes this violation by indicating that it is

then considered as a subcontractor. The defendant having finally admitted to being

13 Emphasis added by the Litigation Chamber.

data controller in its summary conclusions, it argues that since the

March 2021, a privacy policy is present on the site.

56. She also points out that the GDPR does not require this information to be published on the website. It also considers that, given the low number of treatments carried out before COVID, a display in its collection centers was sufficient. She adds that the sudden evolution of its activities since the pandemic justifies that it displays this information on its website.

57. The Litigation Division first notes that the defendant does not bring the proof that the privacy policy was displayed in its centers of sampling. It also considers that the defendant's website cannot be considered as a mere commercial showcase, as the defendant maintains in its findings. Indeed, this website contains a link to the Cyberlab website which allows the analysis results to be consulted. This last website did not contain either more privacy policy. The two websites therefore constitute a tool important operational for the activities of the defendant and not a simple showcase commercial.

58. The G29 in its guidelines on transparency indicates in particular that “Each company with a website should publish a statement or notice on the protection of privacy on its site. A direct link to this statement or notice on privacy should be clearly visible on every page of this site internet under a commonly used term (such as "Privacy", "Privacy Policy", Privacy” or “Privacy Shield Notice”).” 14 Furthermore, he indicates that “all information addressed to a data subject should also be accessible in a single place or in the same document (in paper or electronic) that can be easily consulted by this person if he wishes to consult all the information sent to him. »15.

59. Based on the above elements, the Litigation Division decides that, by not publishing its

privacy policy on its website, the defendant violated Articles 12, 13

and 14 GDPR.

60. She notes that currently, a privacy policy is present on the site

defendant's website.

14 Article 29 Working Party, “Guidelines on transparency within the meaning of Regulation (EU) 2016/679”, version

revised and adopted on 11 April 2018 (Available at: https://ec.europa.eu/newsroom/article29/items/622227), point 11.

15 Ibid., point 17.

II.6. Sanction

61. The Litigation Chamber decides to impose an administrative fine. Like this

clearly emerges from recital 148, the GDPR indeed provides that sanctions, including

including administrative fines, be imposed for any serious violation - therefore

including the first observation of a violation -, in addition to or instead of the

appropriate measures that are imposed.16 The Litigation Chamber demonstrates below

that the violations of articles 5.1.f), 12, 13, 14 and 32 and 35.1 and 35.3 of the GDPR committed by

the defendant are in no way minor violations and that the fine does not

would not constitute a disproportionate burden on a natural person within the meaning of

recital 148 of the GDPR, two cases which would make it possible to waive a fine. The fact

whether it is a first observation of a violation of the GDPR committed by the

defendant in no way affects the possibility for the Litigation Chamber to impose a

administrative fine. The Litigation Chamber imposes an administrative fine in

application of Article 58.2 i) of the GDPR. The instrument of the administrative fine has not

in no way intended to put an end to an offense committed but to do

Effectively enforce GDPR rules. To put an end to an infringement, the GDPR and the

LCA provide for several corrective measures, including the orders cited in Article 100, § 1, 8°

and 9° of the ACL.

62. Having regard to Article 83 of the GDPR and the case law17 of the Court of Markets, the Chamber

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

The Litigation Chamber retains the aggravating circumstances below:

-

-

The fact that the data processed are health data and that they are

large scale (Article 83.2.g) of the GDPR);

The lack of consistency in the explanations of the defendant, who was not

even to determine whether it was a controller or a processor18 and did not

therefore not correctly fulfills the obligations arising from the GDPR, such as the

demonstrate the findings of violation (Article 83.2.k) of the GDPR);

16 Recital 148 provides the following: "In order to reinforce the application of the rules of this Regulation, penalties

including administrative fines should be imposed for any violation of this Regulation, in addition

or in lieu of appropriate measures imposed by the Supervisory Authority under this Regulation. In case of violation

minor or if the fine likely to be imposed constitutes a disproportionate burden for a natural person, a

a call to order may be issued rather than a fine. However, due consideration should be given to the nature,

gravity and duration of the violation, the nature of the violation and the measures taken to mitigate the damage suffered, the

degree of responsibility or any relevant violation previously committed, in the manner in which the supervisory authority

became aware of the breach, compliance with the measures ordered against the controller or sub-

dealing with, the application of a code of conduct, and any other aggravating or mitigating circumstances. The application of

penalties, including administrative fines, should be subject to appropriate procedural safeguards in accordance

general principles of Union law and the Charter, including the right to effective judicial protection and

a regular procedure. [proper underline]

17Court of Appeal of Brussels (Cour des Marchés section), X c. DPA, Judgment 2020/1471 of February 19, 2020.

18 See point 17 above.

-□

The violations noted, although they do not appear deliberate, demonstrate a□

significant negligence in respecting the legislation relating to the protection of□

data (Article 83.2.b) of the GDPR);□

- This aspect is reinforced by the fact that it is only after the intervention of the IS that□

numerous compliance actions have been undertaken (article 83.2.a) of the□

GDPR).□

The Litigation Chamber accepts the mitigating circumstances below:□

-□

-□

The fact that the Respondent was not the subject of violations found by the Chamber□

litigation in the past (article 83.2.e) of the GDPR);□

The defendant remedied the shortcomings noted before the Litigation Chamber□

renders its decision (article 83.2.f) of the GDPR).□

63. On July 25, 2022, the Litigation Division informed the defendant of its intention□

to impose an administrative fine of EUR 25,000. On August 15, 2022,□

the Litigation Chamber receives the reaction of the defendant concerning the intention□

to impose an administrative fine and the amount thereof. The defendant argues□

the following elements:□

has. neither the plaintiff nor any other person suffered damage from the violations□

alleged;□

b.□

the defendant made all the appropriate corrective measures without waiting for the outcome of□

this procedure;□

vs.□

the alleged violations were committed through negligence;□

d.

the defendant has not previously committed violations;

e. The alleged lack of consistency in the defendant's explanations cannot

be reproached because it is due to bad advice and that in any case one cannot

can criticize a person for the way they defend themselves;

f. The main activity consists of fulfilling a mission of general interest, namely

contribute by biomedical analyzes to public health;

g. The defendant's turnover for the financial year in question is certainly (..

EUR) but that the loss of (..EUR) must be taken into account to determine the

financial means of the defendant.

64. In this respect, the Litigation Chamber specifies that arguments b and d of the defendant

have already been considered as mitigating circumstances when submitting the form

fines (see "mitigating circumstances" in point 62).

65. With regard to argument a, the Litigation Chamber recalls that the right to

data protection is a fundamental right of everyone and is included as

as such in Article 8 of the Charter of Fundamental Rights of the European Union. the

controller has no competence to assess the extent of this

law based on the alleged low impact of the breach, whereas the GDPR imposes

positive obligations. Indeed, for many obligations provided for by the GDPR, such as

that the appointment of a DPO, the transparent communication of information, the

implementation of a DPIA etc, the absence of implementation will rarely cause a

direct damage to a person concerned This does not exempt the

controllers of their implementation, especially since the GDPR does not condition

not the imposition of a fine on the controller upon the occurrence of damage.

The Litigation Chamber specifies that argument c, of the defendant, linked to argument e

were retained by the Litigation Division as aggravating circumstances. In

Indeed, the breaches identified demonstrate significant negligence on the part of the

data controller in relation to its obligations relating to the protection of

data. The significance of this negligence is reinforced by the arguments

the defendant's contradictory conclusions. Although a defendant is

obviously

free to choose

the arguments it presents,

the explanations

contradictory may be indicative of insufficient consideration of its

GDPR responsibilities. The Litigation Chamber has previously developed

the contradictory aspects of the defendant's explanations (point 17).

The Litigation Division considers argument f irrelevant in this case. Indeed, only the

public authorities are exempted from the possibility of being fined, in

under article 221, §2 of the law of July 30, 2018 on the protection of persons

physical with regard to the processing of personal data. The defendant

not being a public authority, this article does not apply to it. Furthermore, the fact that

the defendant processes health data on a large scale should induce it to act with

all the more diligence with regard to the protection of this data and constitutes

this title an aggravating factor of the violations found and not a mitigating circumstance.

With regard to point g, the Litigation Chamber recalls that this is indeed the figure

which is used as the criterion for determining the maximum amount of fines

in the GDPR and not the income statement. This choice by the European legislator was made

designed to prevent variations in the income statement from limiting the

ability of data supervisory authorities to impose effective fines. The

Chambre Litigation is however sensitive to the difficult financial situation of the

defendant during the reference year and the significant losses suffered, which may

constitute a mitigating circumstance provided for in Article 83.2.k) of the GDPR. She decides by

therefore reduce the amount of the fine to EUR 20,000.

66. For the sake of completeness, the Litigation Chamber wishes to refer to the Lines

guidelines (Guidelines 04/2022 Guidelines 04/2022 on the calculation of administrative

fines under the GDPR), which the EDPB published on its website on May 16, 2022, for

consultation.

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

disregard it to determine the amount of the fine in this

procedure.

67. All of the elements set out above justify an effective, proportionate sanction

and dissuasive, as referred to in Article 83 of the GDPR, taking into account the criteria

of appreciation it contains. The Litigation Chamber also points out that the other

criteria set out in Article 83.2 of the GDPR are not relevant in this case and do not entail

therefore not an administrative fine other than that determined by the Chamber

Litigation in the context of this decision.

68. In accordance with the foregoing, the Litigation Division finds that it can rely

on the annual figures of medical analysis laboratories to determine the amount of

the administrative fine it intends to impose on the defendant.

69. The Litigation Division refers to the annual accounts filed with the Bank

Nationale de Belgique (BNB) on July 26, 2021, which report a turnover for

the 2020 financial year of (..EUR).

70. The planned administrative fine of 20,000.00 euros corresponds in this case to 0.07% of the

annual turnover of the defendant for the year 2020. The Chamber

litigation refers to the annual accounts filed with the National Bank of

Belgium (BNB) on July 26, 2021, which report a turnover for the financial year 2020

of (..EUR).

71. The Litigation Chamber indicates that the maximum amount of the administrative fine for

a breach is determined by Articles 83.4 and 83.4 GDPR. The amount of the fine

imposed in this decision is significantly lower than the maximum amount provided for (which

could have reached a maximum of EUR 20,000,000), given that the Chamber

litigation took into account all the relevant criteria set out in Article 83.2 of the

GDPR. In addition, the Litigation Chamber assesses the concrete elements of each case

individually in order to impose an appropriate sanction.

III. Publication of the decision

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

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

Data protection. However, it is not necessary for this purpose that the data

identification of the parties are directly communicated.

FOR THESE REASONS,

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

- under articles 100,§1°,13° and 101 of the LCA, to impose a fine of 20,000 EUR

for violations of Articles 5.1.f), 12, 13, 14, 32, 35.1 and 35.3 of the GDPR

- under article 100, §1, 1° of the LCA, to close the file without further action for the findings

remaining.

In accordance with Article 108, § 1 of the LCA, an appeal against this decision may be lodged,

within thirty days of its notification, to the Court of Markets (court

d'appel de Bruxelles), with the Data Protection Authority as defendant.

Such an appeal may be introduced by means of an interlocutory request which must contain the

information listed in article 1034ter of the Judicial Code19. The interlocutory motion must

be filed with the registry of the Court of Markets in accordance with article 1034quinquies of the C.

jud.20, or via the e-Deposit information system of the Ministry of Justice (article 32ter of C.

jud.).

(se). Hielke HIJMANS

President of the Litigation Chamber

19 The application contains on pain of nullity:

(1) indication of the day, month and year;

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

national or business number;

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

(4) the object and summary statement of the means of the request;

(5) the indication of the judge who is seized of the application;

6° the signature of the applicant or his lawyer.

20 The request, accompanied by its appendix, is sent, in as many copies as there are parties in

case, by registered letter to the clerk of the court or deposited at the registry