Litigation Chamber

Decision on the merits 117/2021 of 22 October 2021

File number: DOS-2020-05264

Subject: Complaint about an insecure connection to a hospital website

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

Hijmans, chairman, and Messrs. Dirk Van Der Kelen 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 the "GDPR");

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

ACL";

Seen

the rules of order

interior as approved by

representatives room

the

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 :

The defendant :

X, hereinafter “the plaintiff”;

Y, (formerly referred to as [...], hereinafter "the defendant";

.

.□

.□

.□

.□

.□

I. Facts and procedure□

1. On November 14, 2020, the complainant filed a complaint with the Protection Authority□

data against the defendant.□

2. The plaintiff is a patient at the defendant's hospital institution. The object of the□

complaint concerns the fact that the Internet site (...) belonging to the defendant used a□

contact form and a form for the hospital mediation service. According to□

complainant, the form that could be completed by visitors to the website would be□

sent to the hospital unencrypted. Using an insecure connection□

would allow third parties to gain knowledge of the (health) data.□

3. On November 16, 2020, the complaint was declared admissible by the Front Line Service□

on the basis of articles 58 and 60 of the LCA and is transmitted to the Litigation Chamber in□

pursuant to Article 62, § 1 of the LCA.□

4. On December 16, 2020, in accordance with Article 96, § 1 of the LCA, the request of the□

Litigation Chamber to proceed with an investigation is forwarded to the Inspection Service,□

as well as the complaint and the inventory of parts.□

5. On 26 January 2021, the investigation by the Inspection Service is closed, the report is attached to the□

file and it 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□

regarding the subject of the complaint and concludes that there are violations of Article 32,□

paragraphs 2 and 4 of the GDPR and Article 24, paragraph 1 of the GDPR due to measures□

insufficient to ensure the security of (specific) personal data

which are processed through the defendant's website.

6. The report also contains findings that go beyond the subject matter of the complaint.

The Inspection Service notes, broadly speaking, that it is a question of violations

Article 24(1), Article 38(1) and (3) and Article 39 GDPR

because the Data Protection Officer provided advice to the Managing Director and not

to the board of directors while this body is the highest governing body within

defendant's organization. According to the Inspection Service, the information and opinions that

the Data Protection Officer has provided in accordance with Article 38,

Decision on the merits 117/2021 - 3/12

paragraph 1 and article 39 of the GDPR concerning the security measures for the site

Internet (...) are not convincing enough.

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

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

8. Based on the report of the Inspection Service, the Litigation Chamber decides to split

the case into two separate cases.

9. Pursuant to article 92, 1° of the LCA, the Litigation Chamber will take a decision on the

merits with respect to the subject matter of the complaint.

10. Pursuant to article 92, 3° of the LCA, the Litigation Chamber will make a decision as to

on the merits, following the findings made by the Inspection Service outside the framework

of the complaint.

11. On April 7, 2021, the parties concerned are informed of the provisions as set out

in article 95, § 2 as well as in article 98 of the LCA. They are also informed, under

of article 99 of the LCA, of the deadlines for transmitting their conclusions.

12. For findings relating to the subject of the complaint, the deadline for receipt of

conclusions in response of the defendant was fixed for May 19, 2021, that for the conclusions

in reply of the complainant on June 9, 2021 and finally, that for the submissions in reply of the

defendant as of June 30, 2021.

13. On April 9, 2021, the complainant requested a copy of the file (art. 95, § 2, 3° of the LCA), which

was transmitted on April 12, 2021.

14. On May 11, 2021, the complainant agrees to receive all communications relating to

the case electronically and expresses its intention to make use of the possibility of being

of course, this in accordance with Article 98 of the LCA.

15. On April 20, 2021, the Respondent agrees to receive all communications relating to

the case electronically and expresses its intention to make use of the possibility of being

of course, this in accordance with Article 98 of the LCA.

16. On May 19, 2021, the Litigation Chamber receives the submissions in response from the defendant

concerning the findings relating to the subject matter of the complaint. The defendant asserts that the

Decision on the merits 117/2021 - 4/12

protection of personal data is sufficiently guaranteed thanks to

the legal obligation of secrecy as well as the provisions included in the work regulations

re

the secret,

data minimization and

the

purpose limitation.

Therefore, the defendant declares that data may only be processed in

to the extent that this is necessary in order to achieve the purpose pursued. According to the regulations

of work, non-compliance with the aforementioned provisions is subject to sanctions.

According to the defendant, the complainant does not demonstrate that personal data

concerning him were processed via the website (not secure). For the above reason,

the interest required to lodge a complaint is lacking. In its report, the Service

Inspection refers to another file on behalf of the defendant. The defendant points out

have no knowledge of the contents of the aforementioned file. Therefore, this file is not

relevant in the present case.

17. According to the defendant, Article 24, paragraph 1 of the GDPR has indeed been executed.

The defendant first makes it known that he has launched a project with the ultimate objective of

ISO27001 certification. This certification can, according to the defendant, be considered

as the global standard for information security. Then, still according to the

defendant, it appears from the various contracts that he concluded with subcontractors of

personal data that a detailed analysis has been carried out concerning the

personal data to be processed under the various service contracts

outsourcing. The subcontractor must also always complete a questionnaire on the

basis on which information security and data protection are assessed and

appropriate measures are implemented.

18. Furthermore, according to the Respondent, the Inspection Service wrongly finds that the obligation to

secrecy is not respected by the hospital as the controller and that it has not

nor has it been demonstrated that breaches of the obligation of secrecy could

actually be punished. According to the Respondent, sanctions are indeed

provided for and in the event of breach of professional secrecy by a doctor, dismissal is

even possible. Still according to the defendant, the Inspection Service did not demonstrate that

personal data, let alone health data, are

actually processed via the non-secure form on the website. According to him, he is not

nor demonstrated that unauthorized persons had access to the data

aforementioned. The Respondent claims to have already decided on its own

initiative

the

December 22, 2020 to remove contact forms. The defendant is a

non-profit association and was called [...] at the time the complaint was lodged.

Subsequently, the institution extended its activities to include a rehabilitation center.

Since then, it has continued its activities under the name Y.

19. The Respondent considers that it also meets the requirements of Articles 24 and 32 of the

GDPR as it relates to the internal systems used within the hospital.

Since there is a link between the hospital's website on the one hand and the internal systems

on the other hand, the defendant claims that we opted for two-factor authentication.

According to the defendant, it is clear from the foregoing in particular that security measures

sufficient have indeed been taken.

20. One of the findings of the Inspection Service outside the context of the complaint is that the

data protection officer would not have issued any opinion and would not have reported to

the highest body within the institution on the security measures to be taken within

of the hospital. The defendant believes that he was at all times aware of the importance of the

data protection officer and has therefore always used the latter.

This is evidenced, according to the defendant, by the fact that the delegate was always closely involved

in cases where a subcontract is concluded between the defendant and its

subcontractors. The delegate is also consulted and involved in the development of the

new website in order to ensure that future processing carried out via the website

comply with the legal provisions, according to the defendant. In addition, the protection officer

is part of what is called the Information Security Committee which

fulfills a role of preparation and consultation with regard to the management committee

regarding privacy issues within the hospital. According to the defendant, the director

general is indeed the highest executive power within the hospital. Therefore, he

This is not a violation of Article 38(1) GDPR.

21. Furthermore, the defendant objects that the intention was never that the contact forms

on the website are used to exchange health data. The patient file

mail is indeed very secure according to the defendant. Nor is it a

processing of personal data on a large scale by means of forms

of contact, as established by the Inspection Service. The defendant emphasizes that it should not

neglecting the fact that a form could be completed on the website, a form which

reaches the mediation service and is therefore unrelated to the patient's file.

The Respondent requests that several mitigating circumstances be taken into account, including:

know that no personal data has been accessed by third parties in a way

unauthorized and that when personal data reaches the hospital or

on the hospital's servers, the institution does everything to secure this very

rigorously.

22. The Respondent states that he believes that a security certificate for the Internet form

Should have been implemented sooner when it was pointed out. However, he did not

it has yet been proven that there was a question of prejudice on the part of the person

concerned. There was no access to personal data by persons

not authorised.

23. In addition, several key staff were absent due to the pandemic, which affected

caused a delay in the integration of certain measures. The defendant was not

previously convicted of GDPR violations and started a project with the ultimate goal of

obtaining ISO 270001 certification; he asks that account be taken of the elements

mentioned above as mitigating circumstances.

24. On June 14, 2021, the Litigation Chamber receives the complainant's submissions in reply,

with regard to the findings relating to the subject matter of the complaint. The complainant considers

that the modification of the structure and composition of the hospital should not have led

that the website does not comply with the principles of data protection. In effect,

the GDPR already entered into force in 2018, which implies that the defendant was already in

breach of the GDPR for two years. In response to the Respondent's argument that

which visitors are not obliged to use the contact form, the complainant

objects that website visitors cannot be expected to take

precautions when filling out an online contact form offered by the

respondent. As soon as a form is used, the connection of the website must be

secure. According to the complainant, the fact that confidentiality obligations apply to

collaborators is also relevant, since the personal data which

are transmitted via the contact form are not secure and are exposed to the

risk of being intercepted and read by third parties in network traffic. The complainant does not

does not share the Respondent's view that it would have no interest in introducing a

complaint. The form is indeed available online without being secure and can be

completed and sent by anyone. According to the complainant, the purpose cannot be that he should

search for data subjects who have actually completed the form to

then ask them to file a complaint with the Data Protection Authority.

data.

25. On July 26, 2021, the parties are informed that the hearing will take place on

October 4, 2021.

Decision on the merits 117/2021 - 7/12

26. On October 4, 2021, the defendant was heard by the Litigation Chamber. Despite a

summons in good and due form and a confirmation of his presence, the complainant does not

did not show up.

27. On October 11, 2021, the minutes of the hearing are submitted to the parties.

28. On October 18, 2021, the Litigation Chamber receives from the defendant the remarks

following concerning the minutes: the defendant indicated during the hearing that the

new website was currently online and that the Data Protection Officer

data reported to the audit committee made up of representation from the Board

administration.

II. Admissibility of the complaint

29. The Litigation Chamber first addresses the question of the admissibility of the complaint.

The respondent argues that the complainant has no interest in complaining about the website and the

contact form of the defendant because it is not a processing of his data to

personal character by the defendant. Therefore, according to the respondent, the complaint must

be declared inadmissible or unfounded.

30. Section 58 of the LCA provides that: "Any person may lodge a complaint or

a written, dated and signed request to the Data Protection Authority".

In accordance with article 60, paragraph 2 of the LCA, "A complaint is admissible when it: - is

written in one of the national languages; - contains a statement of the facts and the indications

necessary to identify the processing to which it relates; - comes under the jurisdiction of

the Data Protection Authority".

31. The Litigation Division has already issued the following considerations on this issue in

a previous decision:

"Although the GDPR views the 'complaint' from the perspective of the data subject, in

imposing obligations on the supervisory authorities when a person introduces a

complaint (see Articles 57, 1.f) and 77 of the GDPR), the GDPR does not prevent the right

national gives the possibility to persons other than the data subjects

lodge a complaint with the national supervisory authority. The possibility of a

such referral also corresponds to the missions entrusted by the GDPR to the authorities of

control. In this respect and in general, each supervisory authority: ensures the

Decision on the merits 117/2021 - 8/12

monitoring of the application of the GDPR and compliance with it (Art. 57.1.a) of the GDPR) and

performs any other mission relating to the protection of personal data

personnel (Art. 57.1.v) GDPR)."1 The condition is, however, that the complainant justifies

of sufficient interest.

32. The complainant indicated in the complaint form that he was looking on the website for the

data from his attending physician and then noticed that a connection not

security was used both for the website and for the contact forms.

However, it was not established that the complainant's data had been processed.

33. In addition, the Litigation Division draws attention in this regard to a recent judgment of the

Court of Cassation. In this judgment, the Court established that each data subject who

believes that there is a violation of its rights under the GDPR may file a

complaint to the supervisory authority. However, data subjects including

personal data have not been processed may also introduce a

complaint in some cases. The condition for this, however, is that the data subject

was unable to obtain a specific benefit or a specific service because, by reason of

the existence of the practice constituting a breach as alleged, she refused her

consent to processing2. In this case, according to the Litigation Chamber, one cannot

affirm that it was a question of not being able to use a service, since it existed

also other options such as telephone contact or the possibility of completing

forms on site.

34. As the complainant did not appear at the hearing, the Litigation Division was unable to

obtain further explanations from him. Based on the description of the complaint by

the plaintiff and the exhibits filed, the Litigation Chamber must note that the

complainant, at the time of filing the complaint, was pursuing a general public interest, namely

know the protection of the privacy rights of anyone who visits the site

defendant's Internet and possibly uses the contact forms on the site

Internet. The complainant has not demonstrated that he had any personal interest.

In the given circumstances in which it did not appear that the data to be

personal nature of the complainant had been processed via the contact form or that it

intended to use this contact form, the fact that he was a patient of the hospital in

question is not sufficient to establish that interest.

1 Decision 80/2020 of December 17, 2020 of the Litigation Chamber. See also decision 30/2020 of the Litigation Chamber.

2 Judgment of the Court of Cassation c.20.0323.N/1 of October 7, 2021.

Decision on the merits 117/2021 - 9/12

35. After examination of the complaint in the context of the procedure on the merits, it was therefore found

that the complaint did not meet the conditions of admissibility. The Litigation Chamber

finds therefore that the complaint is and was inadmissible due to the absence

of personal interest. Therefore, the Litigation Chamber will not accept the complaint or the

findings that the Inspection Service subsequently made in the context and in

outside the complaint to impose administrative penalties. The Litigation Chamber

therefore decides to proceed with a classification without further action for technical reasons3.

III.

General considerations

Technical and organizational measures

36. Nevertheless, the inspection report revealed several shortcomings in the manner

whose data the defendant processes. Using the findings from the report

inspection,

the Litigation Chamber wishes to make several considerations

regarding the taking of sufficient security measures to ensure safe processing

of personal data. The Litigation Chamber thus carries out the mission

of the Data Protection Authority which consists of contributing at a level

high data protection.

37. Article 24, paragraph 1 of the GDPR provides the following: “Taking into account 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, the□

controller implements technical and organizational measures□

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

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

necessary."□

38. Article 32 of the GDPR provides the following: "1. Taking into account the state of knowledge,□

implementation costs and the nature, scope, context and purposes of the□

treatment as well as risks, the degree of likelihood and severity of which vary, for the□

rights and freedoms of natural persons, the controller and the processor□

implement the appropriate technical and organizational measures in order to□

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

a) pseudonymization and encryption of personal data; b)□

means to ensure confidentiality, integrity, availability and resilience□

constants of processing systems and services; (c) means to□

3 Discontinued classification policy of June 18, 2021, section 3.1.A.5.□

restore the availability of personal data and access to them in□

appropriate deadlines in the event of a physical or technical incident; (d) a procedure to test,□

to analyze and evaluate regularly□

the effectiveness of technical measures and□

organizational arrangements to ensure the security of the processing.□

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

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

alteration, unauthorized disclosure of personal data transmitted,□

stored or otherwise processed, or unauthorized access to such data,□

accidentally or illegally.□

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

certification mechanism approved as provided for in Article 42 may serve as an element

attesting to compliance with the requirements set out in paragraph 1 of this article.

4. The controller and the processor must take measures to

ensure that any natural person acting under the authority of the controller

or under that of the subcontractor, who has access to personal data, does not process them

not, except on instructions from the data controller, unless obliged to do so by the

Union law or the law of a Member State."

39. According to Article 9 of the GDPR, health data is part of the personal data

special staff. Recital 51 of the GDPR defines this data as being:

"Personal data which are, by their nature, particularly sensitive to the

point of view of fundamental rights and freedoms deserve specific protection,

because the context in which they are processed could create significant risks

for these freedoms and rights." Therefore, the processing of health data must be accompanied

the greatest precautions and all the technical and organizational measures

possible must be taken to protect this data. The main task of a hospital

is to provide medical care. Therefore, it is not unlikely that

patients use these contact forms to share data with the hospital

regarding their state of health. In addition, the form for the mediation service serves

generally to express dissatisfaction and complaints, mainly concerning a

hospital treatment and which are indirectly related to this medical treatment, which

implies that health data is often communicated.

40. As can be seen from the aforementioned articles, the controller is obliged to

implement the necessary technical and organizational measures to guarantee

that the data processing is carried out in accordance with the GDPR. The hospitals whose

main task is to provide medical care regularly deal with

large amounts of health data. They must therefore be particularly vigilant and

ensure that this data is processed in accordance with the GDPR. Bedroom

Litigation emphasizes that personal data relating to health (and

transmission of these) must be sufficiently secure and that the data

must therefore be sent in a form with a level of encryption

sufficiently high from the user's computer to the server which offers a

website with a form. This can be done using a security certificate.

41. In the context of the above, recital 83 of the GDPR specifies: "In order to guarantee the

security and to prevent any processing carried out in violation of this regulation, it

important that the controller or processor assesses the inherent risks

processing and implements measures to mitigate them, such as encryption.

These measures should ensure an appropriate level of security, including

the

confidentiality, taking into account the state of knowledge and the costs of implementation

in relation to the risks and the nature of the personal data to be protected. In the

As part of the data security risk assessment, consideration should be given to

take into account the risks involved in the processing of personal data, such as

destruction, loss or alteration, unauthorized disclosure of personal data

personal transmitted, stored or otherwise processed or unauthorized access

to such data, accidentally or unlawfully, which are likely to lead to

physical, material or moral damage."

Issuance of a report by the Data Protection Officer

42. Guidelines for Group Data Protection Officers 29

provide the following explanations for issuing a report at the highest level

management as referred to in Article 38, paragraph 3 of the GDPR: "If the person responsible for the

processing or the processor makes decisions that are incompatible with the GDPR and

opinion of the DPO, the latter should have the possibility to clearly indicate his dissenting opinion

at the highest level of management and decision makers. Such accountability

directly ensures that senior management (e.g. the board of directors) has

knowledge of the opinions and recommendations of the DPO which are part of the

mission of the latter consisting of informing and advising the controller or

the subcontractor. In this regard, Article 38(3) provides that the DPO "shall

directly report to the highest level of management of the controller

or the subcontractor". Such direct reporting guarantees that the management

Decision on the merits 117/2021 - 12/12

superior (e.g. the board of directors) is aware of the opinions and recommendations

of the DPO which fall within the framework of the latter's mission consisting in informing and

advise the controller or the processor."4 It is therefore clear from the text quoted

above that the data protection officer must be able to do directly

report to the highest level of management. The Litigation Chamber does not exclude that it

could be the general manager in a hospital.

43. The Litigation Chamber recalls that liability as set out in Article 5.2 of the

GDPR implies that the controller is able to demonstrate that it meets

to the obligations as defined in the GDPR.

IV. Publication of the decision

44. 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:

- to close the complaint without further action, by virtue of article 100, § 1, 1° of the LCA.

Pursuant to Article 108, § 1 of the LCA, this decision may be appealed to the

Court of Markets within thirty days of its notification, with the Authority of

data protection as defendant.

(Sr.) Hielke Hijmans

President of the Litigation Chamber

4 Group 29 Guidelines for Data Protection Officers (DPOs) – WP 243 rev.01, p. 18

(https://ec.europa.eu/newsroom/article29/items/612048/en).