1/16

Litigation Chamber

Decision on the merits 22/2020 of 8 May 2020

File number: DOS-2018-02716

Subject: Breach of personal data and obligation to conclude (in time

useful) a subcontract

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

Hijmans, chairman, and Messrs. Frank De Smet and Dirk Van Der Kelen, members;

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

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

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

data protection) (hereinafter the "GDPR");

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

ACL;

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;

Decision on the merits 22/2020 - 2/16

made the following decision regarding:

Y, hereinafter: "the defendant".

1. Facts and procedure

On June 4, 2018, the defendant's data protection officer notifies a data leak to

the Data Protection Authority, pursuant to article 114/1 of the law of 13 June 2005 relating to

electronic communications and in accordance with Commission Regulation 611/2013

European1.

2. On June 6, 2018, the defendant filed an additional notification on this subject with the Autorité

data protection.

3. In its notification, the Respondent mentions that on May 28, 2018, it was informed by telephone of

said data leak by the federal Computer Emergency Response Team (hereinafter "CERT") and that

this CERT notification was confirmed in writing on May 29, 2018.

The data leak took place under the Master IT Service Agreement entered into on June 17, 2014

between the defendant and the Indian company Z (hereinafter "the subcontractor").

By means of this contract, the subcontractor was notably appointed to convert the online store

defendant's existing system, operating on the basis of the Drupal 6 content management system, in a

new online store running on Magento. In addition, the deputy was also asked

dealing with analyzing and solving existing production problems relating to the website.

For the testing of the new online store and the solution of these problems, the subcontractor has placed a

copy of the production database with order history on an Amazon cloud

Web Server (AWS). The subcontractor has activated a web server on port 80 (HTTP) on this AWS and has

allowed free access by applying poor security settings. In addition, the subcontractor has

activated the "Directory Listing" service on this server, thus making it possible to browse the entire

the directory structure on the web server.

1 Commission Regulation (EU) No 611/2013 of 24 June 2013 on measures relating to breach notification

personal data under Directive 2002/58/EC of the European Parliament and of the Council on privacy and

electronic communications, OJ L 173/2.

The personal data of the defendant's customers were thus made available on the Internet between

on March 22, 2018 and May 28, 2018. Forensic analysis of log files revealed that

the data has been viewed and/or downloaded by third parties.

According to the information contained in the notification form submitted by the defendant to

of the Data Protection Authority, this concerned more particularly identification data

(name, address, telephone number), electronic identification data (IP addresses),

National Registry numbers and IBAN numbers of data subjects. The defendant indicates

also in this notification form that the data leak concerns personal data

staff of 32,153 people.

4. By e-mail of June 6, 2018, the Data Protection Authority, after consultation with the Institute

Belgian Postal and Telecommunications Services (hereinafter "BIPT"), asks several questions to the

defendant regarding the data leak and more particularly regarding the nature of this leak

of data, the method of risk assessment used by the defendant, the legal basis

of the processing, the information of the persons concerned and the possible involvement of other States

European members and European supervisory authorities.

5. By email dated June 11, 2018, the Respondent's Data Protection Officer responds to several

of the aforementioned issues.

The defendant transmits a draft notification to be sent to the persons concerned as well as a

draft press release. Furthermore, the defendant specifies that the subcontractor had not

permission to copy data to an environment that is not a

production. The defendant also communicates that no other data protection authority

European was not informed.

6. By e-mail of June 12, 2018, the Data Protection Authority asks a few questions

complementary to the defendant.

More specifically, it asks the defendant to send a copy of the subcontract as well as

as the results of the security audit carried out with regard to the subcontractor. The Authority for the protection of

data also asks whether a data protection impact assessment will be carried out

regarding the risks associated with the management of the defendant's online stores and whether new agreements

specific agreements have been concluded with the subcontractor.

7. Respondent's Data Protection Officer responds to these questions by email from

June 14, 2018.

8. On July 11, 2018, the Board of Directors of the Data Protection Authority decides, pursuant to

of article 63, 1° of the LCA, to seize the Inspection Service of the file given that it observes

serious indications as to the existence of a breach, on the one hand, responsibility for the assessment

of the risk when notifying the breach of personal data, and on the other hand of

the obligation to conclude (in good time) a subcontract.

9. By e-mail of August 10, 2018, the data protection officer of the defendant sends the

answers of the latter to the questions posed by the Data Protection Authority on July 10

2018.

10. By letter dated February 5, 2019, the Data Protection Authority asks several questions

additional to the defendant.

11. On February 22, 2019, the Data Protection Officer of the Respondent transmits the responses of

the latter to questions posed by the Data Protection Authority on February 5, 2019.

12. On August 12, 2019, the Inspection Service sends its inspection report to the Chairman of the

Litigation Division, in accordance with Article 91, § 2 of the LCA.

13. On September 12, 2019, the Litigation Division decided, pursuant to Article 95, § 1, 1° and

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

14. By registered letter of September 12, 2019, the respondent is informed that the complaint

can be dealt with on the merits and, under article 99 of the LCA, it is also informed of the time limit

to present his conclusions.

15. On October 14, 2019, the Respondent filed his pleadings and requested to be heard,

in accordance with article 98, 2° of the LCA.

16. On April 8, 2020, the defendant was heard by the Litigation Chamber, in accordance with article

53 of the internal rules.

17. On April 23, 2020, the minutes of the hearing are sent to the defendant, in accordance with article 54

of the internal rules.

18. On April 28, 2020, the Respondent transmits its remarks, which are annexed to the minutes

hearing, in accordance with Article 54, second paragraph of the internal rules.

2. Legal basis

Article 5.1.f) GDPR

1. Personal data are: (...)

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

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

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

confidentiality);

Article 5.2 GDPR

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

demonstrate that it is respected (responsibility)."

Article 24.1 GDPR

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

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

physical, the controller implements technical and organizational measures

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

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

Article 28.3 GDPR

“3. Processing by a processor is governed by a contract or other legal act under the

Union law or the law of a Member State, which binds the processor with regard to the controller

processing, defines the object and duration of the processing, the nature and purpose of the processing, the type of

personal data and the categories of data subjects, and the obligations and

rights of the controller. This contract or other legal act provides, in particular, that

the subcontractor :

a) processes personal data only on documented instructions from the data controller

processing, including in relation to transfers of personal data to a country

third party or an international organization, unless required to do so under the law of

the Union or the law of the Member State to which the processor is subject; in this case, the subcontractor

informs the data controller of this legal obligation before processing, unless the law

concerned prohibits such information for important reasons of public interest;

b) ensures that the persons authorized to process the personal data undertake to

maintain confidentiality or are subject to an appropriate legal obligation of confidentiality;

c) take all measures required under Article 32;

d) complies with the conditions referred to in paragraphs 2 and 4 to recruit another processor;

e) takes into account the nature of the processing, assists the controller, by means of measures

appropriate technical and organizational measures, as far as possible, to carry out its

obligation to follow up on requests made by data subjects with a view to exercising

their rights provided for in Chapter III;

(f) assists the controller in ensuring compliance with the obligations provided for in Articles 32 to 36,

taking into account the nature of the processing and the information available to the processor;

(g) at the choice of the data controller, delete all personal data or

returns them to the controller at the end of the provision of services relating to the processing,

and destroy existing copies, unless Union law or Member State law requires the

retention of personal data; and

h) make available to the controller all the information necessary to

demonstrate compliance with the obligations provided for in this article and to enable the performance

audits, including inspections, by the controller or another auditor it has

mandated, and contribute to these audits. 4.5.2016 L 119/49 Official Journal of the European Union

With regard to point h) of the first paragraph, the processor shall immediately inform the

controller if, in his opinion, an instruction constitutes a breach of this Regulation

or other provisions of Union law or the law of the Member States relating to the protection of

data."

GDPR Article 32

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

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

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

subcontractor implement the appropriate technical and organizational measures in order to

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

a) pseudonymization and encryption of personal data;

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

constants of processing systems and services;

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

these within appropriate timeframes in the event of a physical or technical incident;

d) a procedure to regularly test, analyze and evaluate the effectiveness of the measures

technical and organizational to ensure the security of the processing. 2. When evaluating the

appropriate level of safety, particular account shall be taken of the risks presented by the

processing, resulting in particular from the destruction, loss, alteration, unauthorized disclosure

authorization of personal data transmitted, stored or otherwise processed,

or unauthorized access to such data, accidentally or unlawfully.

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

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

requirements provided for in paragraph 1 of this article.

4. Finally, the data controller and the processor must take measures to guarantee

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, except on

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

of a Member State."□

Article 33 GDPR□

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

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

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

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

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

it is accompanied by the reasons for the delay.□

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

staff as soon as possible after becoming aware of it.□

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

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

categories and the approximate number of persons concerned by the violation and the categories and the□

approximate number of personal data records concerned;□

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

from whom further information may be obtained;□

Decision on the merits 22/2020 - 8/16□

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

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

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

mitigate any negative consequences.□

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

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

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

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

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

compliance with this article."

GDPR Article 34

"1. When a personal data breach is likely to create a high risk

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

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

2. The communication to the data subject referred to in paragraph 1 of this article describes, in

plain and simple terms, the nature of the personal data breach and contains at

minus the information and measures referred to in Article 33(3)(b), (c) and (d).

3. Communication to the data subject referred to in paragraph 1 is not necessary if one or

the other of the following conditions is met:

a) the controller has implemented the technical protection measures and

appropriate organizational measures and these measures have been applied to the personal data

affected by the said breach, in particular the measures which make the personal data

incomprehensible to anyone who is not authorized to access it, such as encryption

;

b) the controller has taken subsequent measures which ensure that the high risk

for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to

materialize;

(c) the communication would require disproportionate effort. In this case, it is rather carried out a

public communication or a similar measure enabling data subjects to be

equally effectively informed

4. If the data controller has not already communicated to the data subject the breach of

personal data concerning him, the supervisory authority may, after examining whether this

personal data breach is likely to create a high risk, require the

responsible for the processing that it proceeds with this communication or decide that one or the other of the

conditions referred to in paragraph 3 is met".

Decision on the merits 22/2020 - 9/16

3. Motivation

3.1.

As regards the findings relating to the liability of the defendant (Articles 5,

24, 32, 33 and 34 GDPR)

Inspection report findings

19. In its inspection report, the Inspection Service notes that the defendant "gives no

rationale on how it arrives at a concrete risk-based approach such as

imposed (in particular) by Articles 5, 24, 32, 33 and 34 of the GDPR. [Respondent's] referrals to

the "ENISA method for data leaks" and the "CNIL method for a AIPD" are

very general and vague nature; the [respondent] did not act in this case in accordance with Article

5, second paragraph and Article 24, first paragraph of the GDPR". [All passages quoted in this

decision have been freely translated by the Secretariat of the Data Protection Authority, in

lack of official translation].

Defenses of the defendant

20. With regard to this finding of the Inspection Service, the Respondent asserts that he infers from the

joint reading of the aforementioned provisions that this prevention primarily concerns the obligation

to carry out an impact analysis relating to data protection within the meaning of Article 35 of the GDPR

and he argues that according to him, for the treatment in question, he was not obliged to carry out a

such analysis or any other risk assessment.

21. In this regard, he first asserts that the act which gave rise to the data leak took place

before the date of application of the GDPR and therefore Article 35 of the GDPR, which introduces the concept

impact analysis relating to data protection.

22. Second, the Respondent points out that the obligation to carry out such an impact analysis does not

applies only when the processing is likely to create a high risk for the rights and

freedoms of natural persons. He asserts that in this case, the processing activity carried out by the sub-

processing and which was at the origin of the data leak had however been expressly prohibited by the

respondent. The defendant specifies that to test and develop the software, the subcontractor used a

non-production environment in which he could only use data

anonymized. The defendant therefore concludes that he could not be expected to make a

impact analysis concerning an activity of its subcontractor of which it was unaware and for

which he had contractually prohibited the use of personal data.

The defendant refers in this regard to Annex C035A2 entitled "Data Privacy Requirements", attached to the

Master IT Service Agreement concluded in 2014 between the parties, which contains a clause affirming that

"Confidential data cannot be copied from a production environment to a

environment that is not production, unless confidential data is masked".

also refers to article 7 of the subcontract concluded subsequently between the parties, which

provides in particular the following: "The service provider is obliged, for the processing of personal data

staff (…) :

r) to anonymize personal data in a non-production environment at the

using industry-standard technology that still allows the development, testing and

acceptance at the providers or [the defendant]".

23. Respondent also points out that following the June 15, 2018 data leak, it

formally put the subcontractor on notice and attach proof thereof.

24. Furthermore, with regard to this part of the charge, the Respondent asserts that he indeed

taken the appropriate organizational measures to assess the risks and guarantee a level

adequate protection to avoid such risks. He asserts that said Annex C035A2 of the contract

concluded on June 17, 2014 with the subcontractor contained a statement of the risks relating to the processing of

personal data, the main mechanisms to protect personal data

personnel as well as the obligations of the subcontractor in this respect.

25. The Respondent indicates that in accordance with Article 6.2 of the aforementioned Annex, annual audits of the subcontractor were also planned and he attaches the last two audit reports, established by Ernst & Young LLP, as evidence.

26. Finally, defendant argues that it does have a risk analysis method for leaks of data, and that he had it at the time of the 2018 data leak and afterwards. It refers in this respect to its "Data Breach Severity Assessment Method", based on the ENISA method, supplemented in particular by the ISO 31000 and ISO 27005 standards and it attaches documentation to this regard in its submissions in response. The defendant asserts that in addition to this method of analysis risks for data leaks, it also has a general method for analyzing the risks. In this regard, it refers to its internal "Security Risk Management Policy", which is used to assess the risks inherent in all processing activities. The defendant joins this regard documentation as well as an example of analysis based on this method, dating from the 16 September 2017.

27. The Respondent adds that on the basis of the aforementioned valuation method, the risks associated with the flight of data that gave rise to the referral of this file have been assessed. He specifies that within the framework

of this procedure, (the team of) data protection officer, the security manager and the chief compliance officer were successively involved in this risk assessment, after which their analysis was approved by the management committee of the defendant.

28. The defendant pointed out during the hearing that in this case, both himself and the Autorité de la data protection have come to the conclusion that the risk of data leakage should be considered high and that the respondent had taken all necessary measures in this regard2 and that he therefore does not understand on what is based the prevention relating to the non-respect of the responsibility.

Analysis of the Litigation Chamber

29. The Litigation Chamber indicates that the liability of article 5.2 of the GDPR constitutes one of the

central pillars of the GDPR and implies that the controller has the responsibility, on the one hand,

to take proactive measures to ensure compliance with the requirements of the GDPR and, on the other hand

hand, to be able to prove that he took such measures.3

This is what emerges in particular from Opinion 3/2010 relating to the "principle of responsibility" of the Group 29,

which affirms that two aspects must be underlined with regard to this principle:

(i)

(ii)

"the need for the data controller to take measures

appropriate and effective to implement the data protection principles

; and

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

were taken. Accordingly, the manager should provide evidence of

execution of point (i) above".4

30. This responsibility concerns not only the provisions of Article 5.1 of the GDPR but also

the entire GDPR.

31. The above follows from the joint reading of Article 5.2 and Article 24.1 of the GDPR providing

that "Taking into account the nature, scope, context and purposes of the processing as well as the

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

physical, the controller implements technical and organizational measures

2 In particular the notification and additional notification to the Data Protection Authority, a press release

and individual notifications to all concerned.

3 DOCKSEY, C., "Article 24. Responsibility of the controller" in KUNER, C., BYGRAVE, L.A. and DOCKSEY, C. (eds.),The EU G

Data Protection Regulation: A Commentary, Oxford University Press, 2020, (508)557: "The principle of accountability is one of

the central pillars of the GDPR and one of its most significant innovations. It places responsibility firmly on the controller to take

proactive action to ensure compliance and to be ready to demonstrate that compliance".

4 Opinion 3/2010 on the principle of responsibility adopted on 13 July 2010 by the Group 29, p. 9-10,

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_fr.pdf.

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 as necessary."

32. The Litigation Chamber emphasizes that the liability applied to data leaks involves

that a data controller not only has the responsibility to notify data breaches on

where applicable to the supervisory authority and to the persons concerned, in accordance with Articles 33 and 34

of the GDPR, but also that he must be able to demonstrate at any time that he has taken the necessary measures

in order to be able to comply with this obligation.5

33. In its Opinion 3/2010, the Group 29 takes up a non-exhaustive list of "measures of

responsibility" that controllers may take in order to comply with this obligation.

Group 29 mentions in this respect in particular: the introduction of internal procedures, the implementation

written and binding data protection policies, the appointment of a Data Protection Officer

data protection, the development of internal procedures for the management and reporting

effective offenses.6

34. With regard to the evaluation of the effectiveness of these measures, Group 29 refers to the execution

internal and/or external audits as good practice. He specifies in this respect that the methods of

control for the evaluation of the effectiveness of the measures taken must correspond to the risks

specific data processing entails, the amount of data to be processed and the nature

sensitivity of this data.7

35. Finally, it should be stressed that transparency is an integral part of accountability and that

this transparency with regard to the supervisory authorities and the persons concerned as well as the general

public places the data controller in a favorable position with regard to his liability.8

36. The Litigation Chamber considers that on the basis of the documents filed and of its defence, the

defendant demonstrates that in accordance with Article 24.1 of the GDPR, it has taken the measures in this case

technical and organizational and that in accordance with Article 5.2 of the GDPR, it has also

demonstrated, at the request of the Data Protection Authority, that it has taken such measures.

The defendant demonstrates more precisely:

5 FOCQUET, A. and DECLERCK, E., Gegevensbescherming in de praktijk, Intersentia, 2019, 64.

6 Opinion 3/2010 on the principle of responsibility adopted on 13 July 2010 by the Group 29, p. 12-13,

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

7 Same, p. 16-17.

8 Same, p. 16.

-

-

-

-

-

as well as in its contracts with the subcontractor - both in the Master IT Service Agreement

concluded in 2014 only in the subcontract concluded after the entry into force of the GDPR -

, it has taken up the necessary provisions to regulate the processing of personal data

personnel by the subcontractor, and more particularly to prohibit the processing of data

personal character by the latter for the purposes of developing and testing software (in particular

in Appendix C035A2 attached to the Master IT Service Agreement and article 7 of the sub-contract

agreement concluded on June 6, 2018);

that it has developed and documented the required internal risk analysis methods, both

regarding data breaches (the "Data Breach Severity Assessment Method") and

which concerns the assessment of the risks inherent in all processing activities ("Security Risk

Management Policy") and that he also submitted this documentation to the Litigation Chamber,

as well as an example of application of this method;

that it assesses the effectiveness of the procedures and measures it has developed through external audits

annual;

that as soon as he was informed of the data leak by CERT, he acted transparently too

both with regard to the Data Protection Authority and to the persons concerned.

In accordance with Article 33 of the GDPR, the defendant has submitted a notification form as well

that an additional notification to the Data Protection Authority, respectively on the 4th and

June 6, 2018. Pursuant to Article 34 of the GDPR, the Respondent also communicated the

breach of personal data to the persons concerned and has published in this regard a

press release dated June 15, 2018; and

that he formally put his subcontractor on notice on June 15, 2018 following the prohibited processing

and provide proof of it.

37. The Litigation Chamber therefore considers that no violation of the

articles 5.1 f), 5.2, 24.1, 32, 33, 34 and 35 of the GDPR.

3.2.

As regards the findings relating to the obligation to conclude a contract with the

processors (article 28 of the GDPR)

Inspection report findings

38. In the inspection report sent by the Inspection Service to the Litigation Chamber on

August 12, 2019, it is established that the defendant "at the time of the personal data breach

Decision on the merits 22/2020 - 14/16

(during the period between 03/22/2018 and 05/28/2018), had not entered into a contract

with the processor for the processing activity in question. The contract was only concluded by [the

defendant] as of 06/06/2018, as evidenced by the date above the signature of the person

who signed on behalf of [the defendant]. Therefore, in this case, [the defendant] did not act in accordance

in Article 28 of the GDPR".

Defenses of the defendant

39. In its submissions in response and during the hearing, the Respondent asserts in response to this

prevention that on June 17, 2014, a global contract "Master IT Service Agreement" was concluded and that
this contract expressly set out the obligations with regard to the protection of personal data
staff in its article 14.4. Respondent adds that Annex C035A2 titled "Data Privacy
Requirements", forming an integral part of the Master IT Service Agreement, contained obligations
additional information for the subcontractor.9

40. During the hearing on April 8, 2020, the defendant pointed out that the contract concluded on June 17, 2014 with
the subcontractor, and more particularly its article 14.4, met the conditions imposed by law
of 199210, which provided in particular that a contract had to be established between the parties and that it had to
provide that the processor only processes personal data on the instructions of the
responsible for processing and not for purposes other than those defined by the latter.

41. The Respondent adds that this clause was already, however, much wider because it contained
also provisions on data leaks and assistance and which it thus already contained
several elements that were then imposed by the GDPR.

42. Furthermore, the Respondent asserts that when the GDPR came into force, negotiations took place
took place with the sub-contractor and a new sub-contract was drawn up, which was signed on
May 21, 2018 by the subcontractor and June 6, 2018 by the defendant himself. The defendant asserts
that the signing of this contract by the latter was only a formality and that the fact that it
took place only on June 6, 2018 is not relevant since this contract does not contain
obligations only for the subcontractor.

9 Respondent's Response No. 57, p. 15.

10 Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data
(repealed).

Analysis of the Litigation Chamber

43. According to Article 28.3 of the GDPR, processing by a processor must be governed "by a
contract or other legal act under Union law or the law of a Member State, which binds the

processor with regard to the controller, defines the purpose and duration of the processing, the nature
and the purpose of the processing, the type of personal data and the categories of persons
data subjects, and the obligations and rights of the controller." This article also sets out
the mandatory particulars that such a legal document must contain11.

44. The Litigation Chamber finds that the subcontract established by the defendant during
the entry into force of the GDPR contains the mandatory information of Article 28 of the GDPR, but that this
it was not signed by the defendant on the date of entry into force of the GDPR.

45. However, an organization such as the Respondent can be expected to prepare
carefully to the introduction of the GDPR, as soon as the GDPR comes into force, in accordance with
Article 99 of the GDPR, in May 2016. The processing of personal data constitutes indeed
a core activity of the defendant, which also processes such data on a very large scale.

46. Given that the GDPR became applicable from May 25, 2018, the sub-contract
contract concluded between the defendant and its subcontractor had therefore to be signed no later than this
date by both parties.

47. The Litigation Chamber notes, however, that there was an agreement between the parties regarding
this subcontract and that it had been established by the defendant before the date of entry into
force of the GDPR and that it had been signed by the processor.

48. The Litigation Chamber therefore considers that no violation should be found in this case
of Article 28 of the GDPR.

4. Publication of the decision

49. Given the importance of transparency regarding the decision-making process of the Chamber
Litigation, this decision is published on the website of the Authority for the protection of
data, in accordance with Article 95, § 1, 8° of the LCA. However, it is not necessary that at this
end, the identification data of the defendant are directly mentioned.

11 Article 28.3, a) - h) of the GDPR.

FOR THESE REASONS,

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

-

to order the dismissal, pursuant to Article 100, § 1, 2° of the LCA;

Under article 108, § 1 of the LCA, this decision may be appealed within a period

thirty days, from the notification, to the Court of Markets, with the Authority for the Protection of

given as defendant.

(Sr.) Hielke Hijmans

President of the Litigation Chamber