Litigation Chamber

Decision on the merits 48/2022 of 4 April 2022

File number: DOS-2020-02823

Subject: Temperature measurement and processing relating to specific categories

of personal data at Brussels Airport in the context of COVID-19

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

Hielke Hijmans, Chairman, and Messrs. Romain Robert and Jelle Stassijns;

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 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

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 defendant: - Brussels Airport Company SA ("BAC"), whose registered office is located

Boulevard Auguste Reyers 80 - 1030 Schaerbeek, registered under the number

0890.082.292, represented by Me Peter Van Dyck, whose

head office is located Avenue de Tervueren 268A - 1150 Brussels, hereinafter "the

first defendant"; and

- Ambuce Rescue Team SA ("B-Art"), whose head office is located

Bijkhoevelaan 8 - 2110 Wijnegem, registered under company number

.

.□

.□

.□

.□

.□

0878.991.927, represented by Me Evelien Delbeke, whose head office is□

located Natiënlaan 237□

- 8300 Knokke, hereinafter “the second□

defendant".□

I. Facts and procedure□

1. On June 17, 2020, following information published in the press, in accordance with article□

20, §1, 1° of the LCA, the General Secretariat of the Data Protection Authority (hereinafter:□

APD) sent a questionnaire to the first defendant concerning the use of□

thermal cameras at Brussels Airport to measure the body temperature of□

passengers in the context of Covid-19 and any related data processing(s)□

of a personal nature. More specifically, it appears from the above information that the□

body temperature of passengers, both arriving and departing, is measured at the airport□

Brussels Airport using a thermal camera system since June 15, 2020.□

2. By e-mail and by letter dated June 29, 2020, the first defendant replied to the questions□

posed by ODA.□

3. By e-mail of July 6, 2020, the General Secretariat of the APD asked a series of questions□

additional information to the first defendant regarding the legal basis of the processing(s)□

of personal data in the context of taking the temperature (Art. 6 of the GDPR).□

4. On July 9, 2020, the Board of Directors of the Data Protection Authority decided, in□

pursuant to Article 63, 1° of the LCA, to file a file with the Inspection Service, because it□

observed serious indications that temperature screening at the airport

Brussels Airport in the context of COVID-19 could give rise to a breach of the principles

fundamentals of the protection of personal data.

5. By registered letter and e-mail dated July 27, 2020, the Inspection Department, in accordance

to Article 66, §1, 3° of the LCA, addressed to the first defendant a written request

additional information and documents regarding the processing activity

mentioned above.

6. By letter and e-mail dated August 14, 2020, the first defendant sends the Service

of inspection its answers to the questions mentioned above.

Decision on the merits 48/2022 - 3/74

7. On January 19, 2021, the Inspection Service, in accordance with Article 91, §2 of the LCA, submits

its inspection report to the president of the Litigation Chamber, following which the

Litigation Chamber is constituted in accordance with article 92, 3° of the LCA.

In its report, the inspection service makes findings concerning:

-

-

-

-

-

the applicability of the GDPR (Art. 2 GDPR);

the qualification of the controller(s) (art. 4.7 of the GDPR);

compliance with the requirements of proportionality and necessity (Art. 5.1 c), 6.1

c) and e) and art. 9.2 GDPR);

the basis for the lawfulness of the processing (Art. 6 GDPR);

compliance with the obligation of information and transparency (art. 12, 13 and 14

GDPR);

-

carrying out a data protection impact assessment (Art. 35

GDPR); and

- The intervention of the data protection officer (art. 38 and 39 of the

GDPR).

8. On August 19, 2021, the Litigation Chamber decides, pursuant to Articles 95, § 1, 1° and 98 of the

ACL, that the case is ready for substantive processing.

9. By letter dated February 19, 2021, the first and second defendants are informed that the

file is ready to be dealt with in substance and are also informed of the deadlines for

present their defenses pursuant to section 99 of the LCA. The deadline for

receipt of the response from both the first and the second defendants was set for

April 2, 2021.

10. On April 2, 2021, the Litigation Chamber received the response from the second defendant.

11. By letter dated July 6, 2021, the first and second defendants are invited to a

hearing before the Litigation Chamber, in accordance with article 52 of the rules of order

interior.

12. On September 8, 2021, the first and second defendants were heard by the Chamber

Litigation in accordance with article 53 of the internal rules.

13. On September 30, 2021, in accordance with Article 54 of the internal rules, the trial

minutes of the hearing are sent to the first and second defendants.

14. On October 5, 2021, the first defendant sends its observations relating to the trial

aforementioned minutes of the hearing at the Litigation Chamber, which includes them in its deliberations.

Decision on the merits 48/2022 - 4/74

15. On October 6, 2021, the second defendant sends its remarks relating to the trial

aforementioned minutes of the hearing at the Litigation Chamber, which includes them in its deliberations.

16. On February 9, 2022, the Litigation Chamber notified 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 themselves before the penalty is imposed

actually imposed.

17. On February 25, 2022, the Litigation Chamber receives the reaction of the first defendant

intends to impose an administrative fine and the amount thereof.

18. On March 2, 2022, the Litigation Chamber received the reaction of the second defendant to

the intention to impose an administrative fine, as well as the amount thereof.

II. Motivation

II.1. Preliminary considerations

19. The Litigation Division first recalls that this decision concerns the

processing of personal data in the context of the COVID-19 pandemic.

20. In the context of this health crisis, measures have been and are being taken which involve a

unprecedented processing of (special categories of) personal data.

21. The Litigation Chamber understands, given the critical situation, the urgency with

which some of these measures had to be taken by the authorities and bodies

competent and had to be implemented by the data controllers concerned,

as well as the difficulties encountered. It should be noted, however, that this does not carry

prejudice to the fact that compliance with the requirements of the GDPR and other legislation relating to

the protection of personal data, which constitutes an essential protection

of the rights and freedoms of data subjects, must be guaranteed to the fullest extent possible.

possible.

22. The Litigation Chamber recalls that the supervision exercised by the Data Protection Authority

data on technological, commercial or other developments1 and prior notices

of the Knowledge Center do not call into question the obligation of those responsible for

1 Art. 10 of the ACL.

treatment to comply with the legislation in force and that, failing this, they may be

sanctioned by the Litigation Chamber.

II.2. Identification of the disputed processing(s) and applicability of the General Regulations on

data protection (GDPR)

A. Findings of the Inspection Service

23. It appears from the documents in the file and from the investigation report of the Inspection Service that the

disputed treatment consists of a temperature check which, from June 15, 2020, was

carried out daily between 4 a.m. and 10 p.m., in the context of the pandemic of

COVID-19, in front of the entrance to the terminal at Brussels Airport, in two stages2:

1. First line screening: passenger body temperature is measured using

thermal cameras. If the cameras indicate a high temperature (i.e. >= 38°

Celsius), the passenger concerned is first invited to cross the camera lane again. In case of

second observation of a high temperature, the passenger is taken to a

recognized medical service provider at the airport.

2. Second-line control: in a separate medical office, the temperature of the person concerned

is measured again, this time using a hand-held (ear) thermometer. the

passenger is also examined by a B-Art medical expert in order to detect

possible symptoms of COVID-19 and a questionnaire is completed. If, on this basis, the

medical service provider decides that the passenger has symptoms of

COVID-19, access to the terminal is denied. The data subject receives a document

containing the conclusions of the medical expert.

24. In its investigation report, the Inspection Service notes - on the basis of the declarations of

the first defendant - that the first line screening consists of filming the passengers

by means of a camera lane where they are identifiable. The first defendant specifies in this

respect: “The people filmed are briefly identifiable by the operator during the

process. At any time, only the last 15 images are available so that

the operator can ask the persons concerned to cross the camera lane once

second time if the first check indicates an elevated body temperature.3”

2 The documents filed by the first defendant further show that children under the age of 6 were

allowed in the terminal regardless of their body temperature (see Temperature Check Process Description, p.

2).

3Letter from the first defendant dated 06/29/2020, p. 3, point 8 (points 2 and 3).

Decision on the merits 48/2022 - 6/74

25. It is apparent in particular from the documents submitted by the first defendant (see inter alia

Exhibit 3) that images from thermal cameras are immediately converted into

photographs temporarily available, which makes it possible to indicate, for each passenger,

whether the temperature is “green” (< 38° Celsius) or “red” (>= 38° Celsius). This image

static of each interested party - framed in green or red (depending on the temperature

body measured) - is temporarily stored in the volatile memory (RAM) of the terminals

camera work.

26. The first defendant specifies in its answers provided by letter of June 29, 2020 that

the use of these thermal cameras and associated software has been subcontracted to the company

of security X, with which the first defendant has already concluded a framework contract since

2017 regarding access and security controls at Brussels Airport. The first one

defendant attaches to its responses the processing agreement entered into for this purpose with X

in accordance with Article 28 of the GDPR.

27. In its investigation report, the Inspection Service notes, on the basis of the questions

of the first and second defendants, that the second line control implies that

affected individuals, for whom a body temperature of 38 degrees Celsius

or more was observed during the first-line control, were firstly subjected to a

manual temperature control and, on the other hand, that a questionnaire - drawn up by a doctor

specialist - has been traveled with the person concerned in order to carry out a risk analysis

regarding the possibility of infection with COVID-19. This questionnaire was completed and

signed by the person concerned, assisted by a nurse.4 According to the findings of the

Inspection service and declarations of the parties, the questionnaires mentioned above

have been kept on paper (in a ring binder system) and the information that

were extracted from it were also stored in digital form for the purpose of the

contact tracing.5

28. More specifically, it is apparent from the second defendant's explanations that the data

following were collected from the people concerned whose risk of infection by

COVID has been assessed as “high” based on the risk analysis mentioned above

top6:

4 See exhibit 25 (letter B-Art dated 9/10/2020), p. 3.

5 See investigation report, p. 7.

6 See Exhibit 25 (letter B-Art dated 9/10/2020), addendum second line control procedure (p. 10).

29. The second defendant specifies in this respect that these data are recorded in a

Excel file, password protected. This explains in particular that all

records are logged daily in a file, after which this Excel file

is sent by e-mail at the end of the day to an internal employee of the second

defendant; the latter saves this data in a second file (also protected

by a password) in which all the data - collected since the start of the

records - are centralized.

30. According to the statements of the first defendant and its response, the risk assessments

carried out by the second defendant in this regard and the data managed have no

moment were forwarded to the first defendant.7

B. Defenses of the parties

31. Both the first and the second defendants, in their contacts with the Service

of inspection and in their answers, adhere to the finding of the Inspection Service according to

which temperature screening constitutes processing of personal data

within the meaning of the GDPR.8

C. Analysis of the Litigation Chamber

32. According to Article 2.1 of the GDPR, the Regulation applies “to the processing wholly or

partially automated and to the processing of personal data contained or

called upon to appear in a file”.

33. Article 4.1 of the GDPR defines personal data as “any

information relating to an identified or identifiable natural person (hereinafter

referred to as the “data subject”); is deemed to be an “identifiable natural person”

a natural person who can be identified, directly or indirectly, in particular

by reference to an identifier, such as a name, an identification number, data of

7 Reply of the first defendant, p. 6, margin. 4.

8 Reply of the first defendant, p. 9, marg. 13; Answer of the second defendant, p. 7, marg. 15.

location, an online identifier, or to one or more specific elements specific to its

physical, physiological, genetic, psychic, economic, cultural or social identity”.

34. Article 4.2 of the GDPR defines processing as “any transaction or set

operations carried out or not using automated processes and applied to data

or sets of personal data, such as the collection, recording,

the organization, structuring, preservation, adaptation or modification, extraction,

consultation, use, communication by transmission, dissemination or any other form

of provision, reconciliation or interconnection, limitation, erasure or

destruction ".

35. On the basis of the foregoing, the Litigation Division finds that the disputed processing

effectively constitute processing of personal data within the meaning of

Article 2.1 of the GDPR and therefore fall within the scope of the GDPR and the

ODA competence.

36. The Litigation Chamber notes in particular that there are two data processing operations

personal character:

- on the one hand, processing involving the temporary storage of photos

passengers in

the framework of the control of first

line. The

preservation of photos in which the persons concerned are

identifiable, even for a very short period, must be considered

as a processing of personal data. This is a

“processing” within the meaning of the aforementioned article 4.2 of the GDPR, namely the collection

and (brief) preservation “applied to data or sets

of personal data" (in particular "one or more

specific elements specific to the physical identity [...]" within the meaning of Article

4.1 of the GDPR - i.e. a photo). In addition, treatment with

of thermal cameras constitutes an automated processing of data at

personal character within the meaning of Article 2 of the GDPR.

- on the other hand, the processing by which, in the context of the second-hand control

online, the written questionnaires containing the personal data

personnel of the passengers concerned are kept in filing cabinets

as well as in digital form, for a period of five years.

Since this data is stored in filing cabinets, it is

processing of personal data intended for

be included in a file within the meaning of Article 2 of the GDPR (see the files

Excel kept by the second defendant). To the extent that they

are stored in digital form, processing falls by definition

within the scope of the GDPR.

37. With regard to the duration of the treatments mentioned above, it is noted that the control

temperature started on June 15, 2020 and stopped for arriving passengers in

October 2020. In January 2021, this temperature control was also removed for

departing passengers. Moreover, it appears from the documents in the file and the statements of the

parties that the personal data collected as part of the control of

second line are kept for five years.

38. The Litigation Chamber also notes that (some) personal data

personal data processed concern special categories of personal data

within the meaning of Article 9 of the GDPR, and more particularly data relating to the health of

persons concerned. The Litigation Chamber first notes that the temperature

body is measured and processed during first and second line checks. Next,

additional data regarding

the health of the persons concerned are

collected and processed as part of second-line control. The Litigation Chamber

refers in this respect to the questionnaires (aimed at determining the risk profile of the person

concerned) that the second defendant forwarded to the Inspection Service.9 This is

in particular questions relating to the medical history of the data subject and

any symptoms she has or has recently had and/or medical conditions

from which she suffers or has suffered.

II.3. Identification of the controller(s) within the meaning of Article 4.7 of the

GDPR

Findings of the Inspection Service

9 Letter of October 9, 2020 from the second defendant + annexes.

39. On the basis of contacts with the first and second defendants and the analysis of the documents requested, the Inspection Department determines the responsibility for the treatments personal data concerned in this case as follows10:

40. The Inspection Service concludes in particular that, in the context of the performance of the Contract (which was concluded at the end of 2018 and relates to the “delivery of services in the event of medical” and therefore does not, in itself, concern the disputed treatment), the first and the second defendant should be considered joint controllers

Datas. However, with regard to the two (temperature) checks, the Service inspection considers that

the first defendant must be considered as a controller and the second defendant as a processor. In what concerns the “contact tracing” component, the second defendant is qualified as responsible for processing by the Inspection Service.

41. The Inspection Service bases the above analysis on several elements, and in particular on the following findings:

1)

first and second line checks have an identical purpose: the Service inspection finds that the purpose of the two checks is based on the implementation of an element of the Protocol, in particular Chapter 2 of the Protocol: “The measurement of passengers' body temperature. The Inspection Service specifies in this regard that the first line control is a technical control and the second line control a medical control, but that both have the same purpose.11

2)

first and second line processing involves the same data type of a personal nature in the light of Article 9.1 of the GDPR: the Inspection Service

notes in particular that the first and second line controls are all aimed at

10 Investigation report, p. 8-14.

11 Investigation report, p. 10.

two recording body temperature (either using thermal cameras or

using a manual ear thermometer) and that each recording of the

body temperature should be considered as personal data processing

personal. The Inspection Service concludes that in both cases, it is a treatment

personal data within the meaning of Article 9.1 of the GDPR.12

3) the processing was carried out in the same context and at the same place (Brussels

Airport).

4) the legal purpose of the Main Contract concluded between the first and the second

defendant (namely

“emergency medical services”) is not, however,

equivalent to the processing carried out within the framework of the addenda (i.e. within the framework

temperature control). The Inspection Service finds that this is a

extension of the object of the initial contract and that the object and means of the new contract

described in the addenda were determined by the first defendant on the basis of the

Protocol. The Inspection Service concludes that for this treatment - contrary to this

which is the case for the provision of services described in point 2.3 of the Main Contract - the

first and second defendants cannot therefore be considered responsible for the

entirely separate treatment.

Defenses of the parties

42. The first respondent contests the aforementioned analysis of the Inspection Service concerning the

responsibility for processing. The latter considers that it and the second defendant

should be considered as separate data controllers, due to the

contractual agreements between the first and second defendants, on the one hand, and of a series

factual circumstances, on the other hand.

43. First, the First Defendant refers in this regard to Article 19 of the Contract

principal concluded between the first and the second defendant, which provides that the latter

is responsible for the processing of its own personal data 13

44. The first defendant submits that it is apparent from the foregoing that the two parties

contractually agreed that it and the second defendant act as

separate controllers for their own processing.

12 Ibid.

13 Reply of the first defendant, p. 10-11, marg. 16.

45. The first respondent disputes the Inspection Service's assertion that the

Main contract would not be relevant for the disputed processing and that, therefore,

article 19 of this contract would not be applicable. It refers in this respect in particular to

Article 4 of the addendum to the Main Contract, which states: “For the extension of the mandate of

COVID-19 temperature check, the contractor processes personal data

staff for their own needs and under their own responsibility. These data are not in

no cases forwarded to [the first defendant]. [The first defendant] does not wear

no liability in this respect. »

46. The first defendant argues that it is apparent from the contractual agreements mentioned above

above that both parties have agreed that the second defendant determines itself

the purposes and means of its processing in the context of temperature control and that

at no time does the first defendant have access to the data processed by the second

defendant.

47. Secondly, the first defendant refers to a series of factual circumstances

which, according to her, imply that the two parties must be considered as

separate controllers, and in particular that:

-

the processing carried out by the first defendant, on the one hand, and by

the second defendant, on the other hand, constitute two treatments

distinct since the purpose of the processing operations concerned is not the same.

The first defendant considers in particular that the purpose of the

treatment that it carries out itself is to carry out a control

technique of the body temperature of the persons concerned, then

that the purpose of the processing carried out by the second defendant is to

carry out an individual medical assessment.

-

the second defendant itself determined

the means of

treatment it has carried out as part of the second-line control.

In support of its statements, the first defendant refers to:

o Article 2 of the addendum which establishes that: “As part of the measures of

fight against the COVID-19 virus, the Mandate is extended to a new

checking body temperature (2nd line), when reviewing

medical questionnaires and the issuance of a document evaluating the

risk to the passenger (...). »

Decision on the merits 48/2022 - 13/74

o The fact that the second defendant drew up the medical questionnaires

mentioned above completely independently.

o The fact that the second defendant processes health data under the

responsibility of a health professional xxx

o The privacy policy published on the website of the second

defendant, stating: “... In order to provide a quality service, [the

second defendant] will therefore process personal data in

as controller within the meaning of the General Data Protection Regulation.

Data protection (...). »

-

the first defendant had no access at any time to the data of

health treated by the second defendant.14

-

the second defendant, in its correspondence with the Service

inspection, initially presented itself as having to be qualified as

data controller.15

48. In its reply and in accordance with

the analysis of the Inspection Service,

the second

defendant considers that it must be qualified as a subcontractor and that the first

defendant is the controller. However, it appears from the documents in the file that the

second defendant had previously

indicated that it should also be

considered a data controller. The second defendant indicates that

also expressly in his answer.16

49. First, the second respondent argues in its response that it is established that the

processing of personal data that it carries out/has carried out in the context of the

second-line control results directly from the mission entrusted to it by the

first defendant. The second defendant states that the first defendant has

subcontracted its mission of general interest to the first defendant and that the mission subcontracted

treated was threefold: (i) performing a manual temperature check, (ii) reviewing a

medical questionnaire and (iii) issue a risk assessment document to the person□

concerned.□

50. Secondly, the second defendant argues that the fact that a party has a□

certain margin of appreciation in determining the means does not prevent□

14 Reply of the first defendant, p. 13, marg. 20.□

15 Reply of the first defendant, p. 13, marg. 21.□

16 Answer of the second defendant, p. 11-12, marg. 26 et seq.□

that this party is always qualified as a subcontractor. The second defendant argues□

that it is decisive whether or not the party establishes a substantial means and that it cannot□

be responsible for the processing only if it also establishes one or more□

substantial means. The second defendant refers in this respect to the opinions of the Group of□

work Article 29 on Data Protection.□

51. The second defendant emphasizes in this respect that it did not itself determine the□

following elements: the nature of the data processed, the categories of data subjects,□

the frequency of processing, the recipients of the data processed.□

Analysis by the Litigation Chamber□

52. The Litigation Chamber notes that there is no unanimity between the parties regarding the□

responsibility for processing.□

53. In accordance with art 4.7 of the GDPR, the controller must be considered to be:□

the “natural or legal person, public authority, agency or other body which,□

alone or jointly with others, determines the purposes and means of the processing”.□

54. In accordance with Opinion 1/2010 of Working Group 29 and Guidelines 07/2020 of□

the EDPB on the concepts of controller and processor, adopted on July 7□

2021, the capacity of the controller(s) concerned must be assessed in□

concreto.17□

55. The guidelines mentioned above underline that the responsibility for the processing
may be determined by law or arise from factual circumstances. They specify that
the terms of a contract between the parties can also contribute to the qualification of the
controller, but are not decisive.18
56. The Court of Justice of the European Union has also confirmed in its case law that
the identification of the controller(s) requires a factual assessment of the
which natural or legal person determines "the purpose" and "the means" of the
17 See Working Party 29, Opinion 1/2010 on the notions of “controller” and “processor” (version
2.0), February 16, 2010 (WP 169), as specified by the APD in a note entitled “Overview of the notions of responsible
processing/processor in the light of Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April
2016 on the protection of individuals with regard to the processing of personal data (GDPR)
and some specific applications for liberal professions such as lawyers”.
18 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0, 7 July 2021, p. 3.

treatment, by giving a broad definition to the concept in order to protect the persons
concerned.19
57. The Litigation Division finds in this case that the responsibility for the processing
to the disputed processing has not been formally established by law.
58. We can only note that the Commercial Aviation Protocol of 11 June 2020 - which
contains a series of health measures for the aviation sector as part of the fight
against COVID-19 - indicates that the aforementioned measures are applied "by any operator
airport and any airline (...)”. Pursuant to Article 3 of the Royal Decree of 21 June
2004 relating to the granting of the operating license for Brussels-National airport, the
first defendant is the operator of the aforementioned airport.
59. The Litigation Chamber also notes that - as raised by the parties (see above) -
the contracts concluded between the two defendants contain several provisions

relating to the responsibility for processing.

60. First of all, it is noted that the Main Contract concluded between the parties on December 12

2018 provides in its article 19 that “[the second defendant] is responsible for the

processing of its own personal data in the context of the execution of its

mission and must be considered as the controller of this data at

personal character, with the exception of personal data processed by the

Contractor in the relationship to the Principal on behalf of the latter (...)”.

61. With regard to this provision, the Inspection Service is of the opinion that it is not

relevant to the disputed processing and cannot be taken into account, as it does not concern

that the initial object of the contract concluded between the parties (namely the “provision of services in the event of

medical emergency”) and that it predates the contracts between the parties concerning

the disputed treatment (namely taking the temperature in the context of COVID-19). the

Inspection Service concludes that the legal purpose of the Main Contract (as described in

Article 2.3 of said contract) and addenda (concerning second line control in the

temperature control framework) is not the same and that the latter is different in terms of

of objective, design and means. The Litigation Chamber shares the analysis of the

Inspection service according to which disputed processing must be considered and

assessed separately from the initial contracts between the parties, but notes that the addenda

specific - established in the context of the disputed processing operations - also contain

similar provisions concerning responsibility for processing.

19 EU CdJ, 13 May 2014, Google Spain, C-131/12, para. 34.

62. As noted above, temperature control by the first and second

defendant was effectively governed by an addendum to the Main Contract. This addendum

was signed by the parties on July 29, 2020 and was extended four times (see exhibits 11 to

12D first defendant). The addendum mentioned above indicates in its article 4

(“Data Privacy”): “For the extension of the Mandate granted to control the temperature
COVID-19, the contractor [= the second defendant] processes personal data
personnel for its own purposes and under its own responsibility. These data will not be
under no circumstances transmitted to [the first defendant]. [The first defendant] does not wear
no liability in this respect. »20

63. Consequently, the Litigation Division finds that not only in the Contract
principal of December 2018, but also in the addenda extending the mandate
granted to the second defendant in connection with the COVID-19 temperature screening,
the parties have contractually agreed that the second defendant acts as
responsible for the processing of the personal data that it collects and processes in the
framework of the aforementioned control.

64. It should however be noted that, in accordance with the EDPB Guidelines and the
case law of the Court of Justice, the notions of “controller” and “sub-
dealing” are functional concepts and that the contractual clauses do not provide/
may provide only an indication as to the responsibility for the processing, but that
the determination of this liability is a factual rather than a formal assessment and
that it must be established which party actually determined the purpose and means of the processing
disputed within the meaning of Article 4.7 of the GDPR.21

65. The Litigation Chamber therefore identifies the person(s) responsible for the
treatment according to the concrete circumstances of the situation as it arises
in that case.

66. In this regard, the Litigation Chamber notes first of all that after consultation and
collaboration through workshops with the first defendant, the Federal Public Service
Mobility and Transport wrote Chapter 2 (“Measurement of the body temperature of
passengers”) of the Commercial Aviation Protocol, which provides for temperature screening
at airports. The first defendant therefore took an active part in drawing up the

20 Commercial Aviation Protocol June 11, 2020, p. 5. It is the Litigation Chamber which underlines.

21 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0, 7 July 2021, p. 3 (Executive Summary) and p. 9, marg. 12: “(…) the terms of a contract can help identify the controller, although they are not decisive in all circumstances” and “The concepts of controller and processor are functional concepts: they aim to allocate responsibilities according to the actual roles of the parties. This implies that the legal status of an actor as either a “controller” or a “processor” must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a “controller” or “processor” (e.g. in a contract). »

aforementioned protocol. Furthermore, according to the wording of Chapter 2, the task of implementing the measures it provides for was the responsibility of the first defendant, which is the operator of Brussels Airport (art. 3 AR June 2004, see above). In particular, the text of the Protocol states that “(...) the sanitary measures set out in this document are/must be implemented by each airport operator and each airline (...)”.22 This protocol establishes also the purpose of the disputed processing (although in a somewhat ambiguous way, in connection with the provisions of the Ministerial Order of June 5, 2020; see below), namely: "the restart commercial aviation passenger transport activities”.

67. Secondly, it appears from the documents in the file23 that it was the first defendant who contacted potential suppliers and began negotiations for a fever screening solution ". This applies as long as for the processing of personal data in the framework of the first line control as regards the processing of the control of second line. The first defendant notably contacted X for the control by thermal cameras (first line) X and concluded with the latter an addendum to the existing framework contract with the latter in this regard. With regard to the control of the second line, the first defendant asked the second defendant to send a quote to carry out this check. It appears from the documents in the file that the first defendant had already determined the purpose and the means of the mandate and, consequently, the

disputed treatments. It is apparent from the exchanges between the first and second defendants and

of the offers made by the second defendant that the mandate for which an estimate was

requested was "New body temperature check (2nd line) +

examination of the medical questionnaire + submission of the “risk assessment” document to the

passenger”.24

68. The first defendant therefore initiated the disputed processing operations and decided to subcontract

part of the temperature check to the second defendant after performing a

preliminary market study and requested an estimate from the second defendant.

69. However, it appears from the analysis of the file that the second defendant, with regard to the

processing of personal data in the context of second-line control, a

it also determines independently at least certain means within the meaning of Article 4.7

of the GDPR.

22 It is the Litigation Chamber which underlines.

23 See also the Inspection Service investigation report, p. 9.

24 See letter from the second defendant dated 09/30/2020 addressed to the Inspection Service (appendices 3 and 4; estimate).

70. This is deduced first of all from the fact that, in its replies to the Inspection Service, the second

respondent indicates that "the concrete terms of the mandate granted by [the first

defendant] were determined by [the second defendant] ... These procedures

relating to the disputed processing are set out in Appendix 11”.25

71. It emerges from the analysis of the aforementioned Annex 11 that the aforementioned internal procedure of the second

defendant provided, in particular, which specific categories of personal data

personnel would be collected during the second line control and how and under what

form they would be retained (point 8.1.3.1 of the procedure) and that the name and number of

flight of people with a high risk profile would be passed on to the company

airline concerned (point 8.1.3.4). It appears from the documents in the file and from the hearing that the

second defendant, on its own initiative, sought the opinion of the National Council of the Order
doctors in this regard in order to obtain confirmation that it was not a violation
professional secrecy. Furthermore, it is also apparent from the file that the second
defendant determined the retention period to be applied to personal data
personnel collected and processed during the second line control. It indicates in particular
in its letter dated October 9, 2020 addressed to the Inspection Service:
“Data relating to health must be retained under Belgian law
(obligation to keep a record, Patients' Rights Act). It was decided to set a deadline of
retention of 5 years, period dictated by the possibility for the passenger to initiate an action in
liability against [the second defendant] (5 years being the limitation period for a
extra-contractual action)”.26
72. It should be noted that in its guidelines, the EDPB makes a distinction between
“essential” and “non-essential means” of processing and specifies in this respect that the
determination of the essential means is inherent in the status of controller.
The EDPB defines as essential means those means which are closely related to the purpose and
to the scope of the processing and which determine whether the processing in question is lawful, necessary
and proportionate. The EDPB gives here a non-exhaustive list of examples of essential means
processing of personal data, indicating: the type of data to be processed
personal data processed, the retention period of the personal data
collected and processed and the categories of data subjects. Non-essential means,
according to the EDPB, relate rather to purely practical aspects of the processing, such as the
choice to use a particular type of hardware or software or more security measures
25 Ibid, p. 2.
26 See letter from the second defendant dated 09/10/2020 to the Inspection Service, p. 5.

detailed.27 The determination of these latter elements can also be left to a

subcontractor, in accordance with the guidelines mentioned above.

73. It is apparent from the foregoing that (contrary to what she asserts in her reply) the second defendant actually established or, at the very least, controlled a series of essential means of processing - namely, the exact categories of personal data personnel collected through medical questionnaires, the retention period and (one) of the recipients of the data (i.e. airlines). It makes sense in insofar as the second-line check is of a medical nature and is carried out by the health personnel, while first-line control is more technical in nature and is carried out by security personnel.

74. The Litigation Division notes, however, that the first defendant also established, in addition to the purpose (see above), the essential means of the disputed processing, and this also applies to processing within the framework of second-line control. It comes out in made of the documents in the file that, when the specifications were requested at the second defendant, it was already planned how the second-line control would be carried out, find out through a body temperature check, a medical questionnaire and the delivery of a risk assessment document to the data subject.

75. With regard to processing under the second line of defence, the first defendant indicates in its reply that the personal data processed by the second defendant were not forwarded to it (marg. 20). She says she doesn't know how many medical questionnaires have been completed and how (how long) they are preserved. However, the EDPB stresses in its Guidelines 7/2020 that a controller does not necessarily have to have access to the personal data personnel processed to qualify as data controllers.28 Accordingly, the above argument of the first defendant cannot be accepted.

76. Based on the foregoing, the Litigation Chamber first concludes that the first

defendant must be considered the sole data controller within the meaning of

Article 4.7 of the GDPR for the processing of personal data in the context of

first-line screening, i.e. measuring the body temperature of passengers

using thermal cameras, and

the grip and

brief storage of images

photographs of the persons concerned. Secondly, the Litigation Chamber

27 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0, 7 July 2021, p. 15,

marg. 40.

28 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0, 7 July 2021, p. 15,

Executive summary, p. 3.

Decision on the merits 48/2022 - 20/74

finds that the first and second defendants must be considered as

Joint controllers within the meaning of Article 26.1 of the GDPR for the processing

of personal data in the context of second-line control. In

Consequently, in this capacity, they are both bound by the obligation to

responsibility contained in Articles 5.2 and 24 of the GDPR to ensure compliance with

principles and provisions of the GDPR.

77. Article 26.1 of the GDPR defines

joint controllers such as

follows: “Where two or more controllers jointly determine the

purposes and means of processing, they are joint controllers”. The

aforementioned provision further specifies that they define in a transparent manner their

respective responsibilities in respect of compliance with the obligations of the head of this regulation,

in particular with regard to the exercise of the rights of the data subject and their

respective obligations to provide the information referred to in Articles 13 and 14 of the GDPR, by

through an arrangement between them, except if and insofar as the responsibilities
respective controllers are established by a provision of the law of
Union or Member State law applicable to controllers.

78. In its guidelines, the EDPB specifies, with regard to joint liability in
matter of treatment, that it can take different forms. Thus, it should be noted that
the joint determination of the purpose and means of the processing in question can be
carried out either by means of a joint decision, or following convergent decisions
taken by two or more entities with regard to the purpose and/or the (essential) means
treatment.29

79. In the present case, it is established that there are at the very least convergent decisions of the first
and the second defendant as regards the determination of the purpose and the
means of processing personal data collected in the context of the
second line control.

80. Finally, the Litigation Chamber notes, as the Inspection Service did in its report
of investigation, that the second defendant acts as the sole controller of the processing of
data with regard to the derivative processing activity “contact tracing” and must
therefore ensure compliance with the aforementioned provisions for this processing activity.

II.3. Compliance with the principle of necessity and the lawfulness of processing (Art. 5.1, 6.1 e) and 9.2 g) of the
GDPR)

29 EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.0, 7 July 2021, p. 19,
marg. 54.

Findings of the Inspection Service

81. In its investigation report, the Inspection Service notes that the first respondent
violates the necessity requirements contained in Articles 5.1 c) and 6.1 c) and e) and 9.2 of the
GDPR by choosing not to carry out temperature checks without processing

personal data.

82. According to the Inspection Service, it should be checked whether the processing meets a need

medical and legal.

o As for medical necessity, the Inspection Service specifies that it is not

It is not up to the DPA to comment on this point, but notes that the medical necessity of the

second-line control is disputed by various authoritative sources. the

Inspection service refers in this context to the information on

the website of the World Health Organization (WHO)30, in the report

technical support from ECDC (European Center for Disease Prevention and Control)

of June 12, 202031, on the advice of the French supervisory authorities and

Dutch authorities32 and the common position of EASA and ECDC of 30 June

2020.33

o With regard to legal necessity, the Inspection Service indicates any

firstly, that it follows from the text of Article 9.2 i) of the GDPR that, in addition to the need

medical condition (which is disputed), a legal necessity must exist and have a basis

legal. With regard to this last point, the Inspection Service is of the opinion that

neither the Protocol nor the other standards invoked contain an obligation

to organize a temperature control in two lines and that consequently, the

conditions of Article 9.2 i) of the GDPR are not met (or any other reason

applicable exemption).

With regard to this legal necessity, the Inspection Service specifies in

besides that it must be assessed in the light of the criteria established by the case law

with regard to Article 8 of the ECHR and Article 22 of the Constitution (see below

item II.4).

30 Investigation report, p. 17.

31 Ibid, p. 18.

32 Ibid, p. 19-20.

33 Ibid, p. 21.

Defenses of the parties

83. As regards the necessity, the first respondent disputes the findings of the Inspection Service and considers that the principle of necessity contained in Articles 5.1, 6.1 and 9.2 of the GDPR is well respected. The first defendant submits, in particular, that:

▪ at the time the temperature check was performed, there were no other (safe) alternatives to achieve the same goal. The first defendant argues that there were no rapid tests and that individual manual temperature control would have caused queues, which would have created a dangerous situation;

▪ the temperature control system in 65 other European airports and not Europeans, was implemented as part of the fight against COVID-19;

▪ the reference made by the Inspection Service to the opinions of the WHO and the ECDC is not relevant, since the first defendant was only applying the Protocol which gave it was applicable and therefore had no choice in the matter;

▪ the Inspection Service wrongly considers that it could opt for a control other than a two-line control. the first defendant refers in this respect to the lines EASA guidelines and indicates that they prescribe the following:

“The process should aim to identify passengers whose skin temperature is equal or above 38° Celsius, unless otherwise specified by national health authorities. For passengers with elevated skin temperatures, thermal screening must be repeated at least once for confirmation. Passengers with a

elevated skin temperature should be referred for secondary evaluation by a

health specialist or follow the agreed monitoring protocol”.

▪

temperature control was stopped as soon as it was no longer necessary (in particular in

due to negative COVID tests required for departing passengers).

84. The second defendant disputes - with regard to the second-line control to which

it proceeded - the findings of the Inspection Service according to which the requirement of

necessity would have been violated. More specifically, she asserts that:

▪

the EASA position (see above) and a study carried out in Taiwan on May 9, 2020

show that this type of control can detect 32.7% of COVID-19 infections.

19;

▪

the EASA directive also prescribes that in the event of temperature control by

thermal cameras, a second line check must be carried out;

▪

the task of the second defendant consisted solely of carrying out the control of

second line and that this task consisted in controlling the measurement of the cameras

thermal, on the one hand by manually measuring the body temperature again

Decision on the merits 48/2022 - 23/74

and, on the other hand, by evaluating other (possible) symptoms on

the basis of a

medical questionnaire. The second defendant argues in this respect that this control

of second line has made it possible to avoid proceeding solely on the basis of one of the

possible symptoms of COVID-19, namely fever;

▪

second-line medical control preserves the rights and freedoms of individuals

concerned and can be considered as a data protection measure by

its design;

▪

second control

online is required for a full assessment and

medically based risk profile of passengers.

85. As regards the lawfulness of the processing, it must be noted that the first

respondent does not expressly indicate in its response on what legal basis

article 6.1 of the GDPR it is based for the disputed processing. During the hearing, she

however, clarified that it was based on Article 6.1 e) of the GDPR (need to perform a

mission of public interest or subject to the exercise of official authority) combined with Article 9.2

g) of the GDPR as grounds for lawfulness and exception. It specifies that this last provision

must be interpreted as meaning that, in addition to an important reason of public interest, it is necessary to

demonstrate a legal obligation under the law of a Member State or European law.

86. In this regard, the first defendant recalls, on the one hand, that Article 9.2, g) of the GDPR

authorizes the processing of data relating to health if “the processing is necessary for

important reasons of public interest on the basis of Union law or the law of a State

member (...)". It specifies that the fight against the COVID-19 pandemic must be considered

as falling within the scope of the aforementioned provision and refers, in this regard,

in recital 46 of the GDPR which indicates, as an example of grounds of public interest

important: “(...) where the processing is necessary for humanitarian purposes, including

monitor epidemics and their spread (...)”.

87. Both the first and the second defendants invoke the lawfulness of the processing operations:

1)

the Commercial Aviation Protocol of the Minister of Mobility and Transport

dated June 11, 2020. The first defendant specifies in this regard that the database

of the aforementioned protocol is the Ministerial Order of March 23, 2020 on

emergency measures to limit the spread of the COVID-19 coronavirus (such as

amended several times), on the one hand, and the law of 31 December 1963 on the protection

civil law (as replaced by the law of May 15, 2007), on the other hand. The first one

defendant mentions in this regard that the Council of State, in a judgment of

October 30, 2020, approved the use of the aforementioned standards as a legal basis

to take action in the fight against COVID-19. In what

Decision on the merits 48/2022 - 24/74

concerning this document, the first defendant asserts that the objective of the protocol

was to ensure the protection of the health of passengers at the airport. She asserts that

this includes the obligation to carry out temperature checks - the treatment

litigious ; and

2)

the Royal Decree granting the operating license. The first defendant points out that

Article 4 of the aforementioned RD stipulates that: “The holder provides for the airport of Brussels-

National (...) 4° the maintenance of safety and security on the ground (...). " The first one

defendant asserts that it is obliged to comply with this AR and argues that the only

how it could comply with this provision in the context of the

COVID-19 pandemic was to conduct a temperature check.

Analysis of the Litigation Chamber

1. General

88. The Litigation Chamber recalls that the processing of personal data is not

lawful only if carried out in accordance with Article 6.1 of the GDPR.

89. In view of the fact that it has been established in the present case (see above) that the supervisory system

also involves processing special categories of personal data

- in particular data on the health of the persons concerned within the meaning of Article 4.15 of the GDPR - controllers must also demonstrate that one of the grounds for derogation from the fundamental prohibition to process this type of personal data, listed in Article 9.2 of the GDPR, is applicable. As the Litigation Chamber has already indicated34, the processing of special categories of personal data within the meaning of Article 9 of the GDPR shall be based on Article 9.2 of the GDPR read in conjunction with Article 6.1 GDPR. This has been established by the European Commission and the EDPB35 and is also confirmed by recital 51 of the GDPR, which indicates, with regard to the processing of special categories of personal data, that "in addition to the requirements applicable to this processing, the general principles and the other rules of this

34 See Decision on the merits 76/2021, paragraph 33, https://www.autoriteprotectiondonnees.be/publications/decision-as-to-fund-n-76-2021.pdf.

35 See on this point GEORGIEVA, L. and KUNER, C., “Article 9. Processing of special categories of personal data” in KUNER, C., BYGRAVE, L.A. en DOCKSEY, C., The EU General Data Protection Regulation (GDPR). A Commentary, Oxford University Press, Oxford, p. 37: “The Commission has stated that the processing of sensitive data must always be supported by a legal basis under Article 6 GDPR, in addition to compliance with one of the situations covered in Article 9(2). The EDPB has also stated that ‘If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. and exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6’.

Regulation [must] apply, in particular as regards the conditions for the lawfulness of the treatment. »36

2- With regard to the application of Article 9.2 g) combined with Article 6.1 e) of the GDPR in the present case

90. The Litigation Chamber recalls that, in order to validly rely on the ground for derogation the prohibition to process special categories of personal data provided for

in Article 9.2 g) of the GDPR, the controller must demonstrate that:

(i)

(ii)

there is an important reason of public interest;

a ground is present in Union law or the law of a Member State for the

disputed processing, ensuring proportionality in relation to the objective pursued,

respecting the essence of the right to the protection of personal data and

providing for appropriate and specific measures to protect the rights and interests

fundamentals of the data subject; and

(iii)

the disputed processing is necessary for the important reason of public interest

mentioned above.

91. As specified above, for the processing of special categories of personal data

personal nature, Article 9 must be applied in conjunction with Article 6.1 of the GDPR. The

controllers claim to rely in this case on Article 6.1 e) of the GDPR. The

Litigation Chamber recalls that the use of the ground of lawfulness contained in the provision

above implies that the controller must be able to demonstrate that:

i)

ii)

the processing is necessary for the performance of a task in the public interest or

relating to the exercise of public authority; and

the processing in question is necessary for the performance of the mission mentioned

above.

92. With regard to the first constituent element of Article 9.2 g) of the GDPR, in particular

the existence of an “important public interest”, the Inspection Service, in its report

investigation, does not call into question the existence of such an interest in the present case. In this regard, the

Litigation Chamber considers that

one can indeed consider that there was

an “important public interest” within the meaning of Article 9.2 g) of the GDPR. The Litigation Chamber

is of the opinion that there is no doubt that (the fight against) the COVID-19 pandemic must be

considered as such. The Litigation Chamber recalls that the assessment of the existence or

not of significant public interest involves balancing the public interest, on the one hand, and

36 It is the Litigation Chamber which underlines.

the risks to the rights and freedoms of the persons concerned, on the other hand.37 The Chamber

Litigation recalls that the threshold for satisfying the aforementioned criterion must be assessed

strictly, but considers that in the present case it can be accepted that this criterion was met.

This is, moreover, expressly stated, as the defendants also point out,

in recital 46 of the GDPR, which mentions that “monitoring epidemics and their spread”

is an “important reason in the public interest”.

93. The second constituent element concerns the existence of a legal basis in “the law

of the Union or the law of a Member State, which must be proportionate to the objective pursued,

respect the essence of the right to data protection and provide for appropriate measures

and specific for the safeguard of fundamental rights and the interests of the person

concerned" within the meaning of Article 6. 1 j° 9.2 g) of the GDPR.

94. In accordance with Article 6.3 of the GDPR, read in the light of recital 41 of the GDPR, the

processing of personal data which is necessary for the performance of an obligation

law38 and/or the performance of a task in the public interest or in the exercise of authority

public authority vested in a data controller39 must be governed by regulations

clear and precise, the application of which must be foreseeable for the persons concerned.

95. Article 6.3 of the GDPR is more specific: “The basis for the processing referred to in paragraph 1,

points c) and e), is defined by: a) Union law; or (b) the law of the Member State to which the

controller is submitted. The purposes of the processing are defined in this

legal basis or, with regard to the processing referred to in point (e) of paragraph 1, are

necessary for the performance of a task in the public interest or relating to the exercise of authority

public authority vested in the controller. »

96. Recital 41 of the GDPR specifies in this regard: “Where this Regulation refers

to a legal basis or legislative measure, this does not necessarily mean that

the adoption of a legislative act by a parliament is required, without prejudice to the obligations

provided for under the constitutional order of the Member State concerned. However, this basis

legal or legislative measure should be clear and precise and its application should

be foreseeable for litigants, in accordance with the case law of the Court of Justice of

European Union (hereinafter referred to as the “Court of Justice”) and the European Court of

human rights. Furthermore, according to article 22 of the Belgian Constitution, it is necessary that

37 GEORGIEVA, L. en KUNER, C., “Article 9. Processing of special categories of personal data” in KUNER, C., BYGRAVE,

L.A. en DOCKSEY, C., The EU General Data Protection Regulation (GDPR). A Commentary, Oxford University Press, Oxford,

p. 379.

38 Art. 6.1.c) GDPR

39 Art. 6.1.e) GDPR

the “essential elements” of the processing are defined by means of a formal legal standard

(law, decree or ordinance).40

97. As regards the legal basis invoked by the defendants, it should be noted that

neither the Royal Decree granting the operating license, nor the Ministerial Decree, nor the Security Act

civil law regulate the disputed processing as such. This treatment is provided for by the

Commercial Aviation Protocol, adopted by the Federal Public Service Mobility and

Transport (DG Aviation), after negotiations with the sector concerned. This last point

emerges from the wording of Article 1, 3° of the Ministerial Order: “protocol”: the document

determined by the competent minister in consultation with the sector concerned". That is what
also emerges from the documents in the file and, inter alia, from the e-mail sent by the cabinet of the
competent minister to airport operators, airlines and authorities
dated June 11, 2020. The Litigation Chamber recalls that, in the context of
Article 6.3 of the GDPR and recital 41, consultation and collaboration with the sector
do not pose a problem in themselves, provided that the legal obligation and/or the mission of interest
public are explicitly provided for in regulations issued by the authorities. This
however, was not the case in this case.
98. Indeed, the documents and standards to which the defendants refer cannot be
considered as a law according to the qualitative criteria established by the case law of the Court
of Justice of the European Union and of the Constitutional Court. The Litigation Chamber
refers in this respect in particular to the Privacy International judgment of the Court of Justice dated
October 6, 2020, in which the Court indicates that the legislation in question must contain
clear and precise rules "on the scope and application of the measure concerned, so that
persons whose personal data are in question have guarantees
adequate that these data will be effectively protected against any risk of misuse". The
Court adds: "These rules must be legally binding in domestic law and
must specify, in particular, the circumstances and conditions under which a measure
providing for the processing of such data can be taken, thereby ensuring that any
interference is limited to what is strictly necessary. (...) These considerations apply in particular
when it comes to protecting a particular category of personal data,
know sensitive data. »
99. In view of the aforementioned standards, the first respondent indicates in its response that the
Council of State, in its judgment of October 30, 2020, "[has] approved the legal basis of Article 4
of the Law of December 31, 1963 and Articles 181, 182 and 187 of the Law of May 15, 2007.
40 "Everyone has the right to respect for his private and family life, except in the cases and under the conditions established by

the rule referred to in Article 134 guarantee the protection of this right. »

Decision on the merits 48/2022 - 28/74

should be noted, however, that the judgment mentioned above does not concern the use of

this legislation as the legal basis for the processing of (special categories of)

personal data and in no way relates to an assessment of the standards

mentioned above in light of the GDPR. The judgment relates to the closure imposed on

restaurants and drinking places in the context of COVID-19 and, as such, it is therefore not

not relevant to this case. In addition, the judgments of the Council of State concern the

legality of the measures imposed by Ministerial Orders, which have a normative character. Now, this

is not at all the case for the Protocol in question.

100. This was also confirmed by the Council of State in its opinion no. 69.253/AG of 23 April

2021, issued by the General Assembly of the Legislation Section, in which he states:

“One of two things: either the protocols have no regulatory character, but in

In this case, the concrete measures they contain are not binding, the protocols

cannot derogate from the ministerial decree and their respect cannot be controlled or

maintained by the intention of a public action in the event of non-compliance; either the protocols

are indeed regulatory and the measures they contain are indeed

constraining, but in this case, these measures must appear in decrees of

competent authority in the matter”.41

101. The Council of State, in response to a question from the Minister's delegate, declares the following in

the same opinion with regard to the legal value of the protocols:

“The protocols and guides provide an indicative assessment framework. The protocols and

the guides can only concretize the regulatory measures, as provided for in the MA,

but are not themselves regulatory. »42

102. The Litigation Chamber also refers to a judgment of the French Council of State relating to the

processing of special categories of personal data by means of

thermal cameras without a valid legal basis, in which the latter indicated "it is not
possible to estimate that the legal conditions for the processing of personal data of
provided for in g) under 2. of Article 9 of the GDPR are met, for lack of text governing
the use of thermal cameras deployed by the municipality and specifying the public interest that
may make it necessary".43

41 Legislation Section of the Council of State, Opinion No. 69.253/AG of April 23, 2021, p. 22, marg. 20.3, http://www.raadvst-
consetat.be/dbx/avis/69253.pdf.

42 Ibid., p. 42, marg. 20.2.

43 Free translation: "it is not possible to consider that the legal conditions for the processing of personal data of
provided for in g) under 2. of Article 9 of the GDPR are met, for lack of text governing the use of thermal cameras
deployed by the municipality and specifying the public interest which may make it necessary".

103. On the basis of the foregoing, the Litigation Division finds that the Protocol of
commercial aviation does not constitute a valid legal basis within the meaning of Article 6 of the
GDPR due to its lack of binding character in Belgian law.

104. Even if this instrument were to be considered binding, quod non, it should be
find that the protocol in no way imposed on the defendants the execution of the processing
litigious. This is particularly evident in the following:

-

the Protocol itself states: "The measurement of body temperature
passengers so that they can travel with a "passport
immunity" is not recommended by EASA and ECDC. EASA
recalls that the relevance of this measure is not supported by the
current scientific knowledge about SARS-CoV-2. However,
EASA and ECDC monitor scientific developments and, where appropriate,
will update their recommendations if an appropriate test becomes

available. »44

The version of the protocol dated June 11, 2020 does not mention anything concerning

Brussels Airport in Zaventem. However, he specifies:

“At the request of the airlines operating flights there, the airport of

Charleroi (Brussels South Charleroi Airport) has however decided to set up

tests to measure body temperature for people

entering the airport building. The airport guarantees that the chosen method

will not cause any delay or concentration of people at the entrance to its

infrastructure. »

In this regard, the version of July 31, 2020, however, mentions with regard to

Brussels Airport:

“Brussels National Airport has also informed us that it has been decided to

set up tests to measure body temperature for children

people entering the airport building. » 45

-

the first defendant itself took

initiative to stop

the

disputed treatment. This is what emerges from the letter sent to the APD on

January 21, 2021, which states: “We hereby wish you

44 Commercial Aviation Protocol, June 11, 2020, p. 5. It is the Litigation Chamber which underlines.

45 Ibid, version of July 31, 2020, p. 5. It is the Litigation Chamber which underlines.

inform that Brussels Airport Company (BAC) has decided to end the

temperature control due to the changing situation. »

The Litigation Chamber considers that the above elements demonstrate that

the Protocol was not binding and could not constitute a basis

legal basis for the disputed processing.

105. The above is also confirmed - despite what is said in its answer - by the

first defendant in its impact assessment relating to data protection (DPIA;

see below). The latter itself mentions the following as one of the risks identified for the

rights and freedoms of natural persons: “currently there is no legal framework. No law

exists that obliges or allows airports to check the temperature of passengers”.46 The

first defendant itself qualifies the impact of the aforementioned risk as “critical”. In the

initial version of the DPIA sent to the Inspection Service, the first defendant does not

does not provide a solution to this identified risk. In the version of the DPIA submitted to the Chamber

Litigation appended to the response, the following is indicated under “risk solution”: “Brussels

Airport bases itself on a Ministerial Decree (AM of March 23, 2020 containing measures

to limit the spread of the coronavirus COVID-19) and FAQ of the Center de

National crisis and a Protocol drafted by the Security Council for the aviation industry in

Belgium”.47 It follows from the foregoing that the first defendant, as

data controller, was aware that the processing it was carrying out was not

based on a valid legal basis. However, on the basis of the liability provided for in

Article 5.2 of the GDPR, it is up to the controller to ensure that a reason for

valid and adequate lawfulness within the meaning of Article 6.1 of the GDPR exists from the start of the processing

litigious.

106. As already mentioned above, the Litigation Chamber emphasizes that the standards

legal claims invoked by the defendants do not satisfy the conditions of Article 6.3 of the

GDPR and the case law of the Court of Justice, for the reasons set out below.

The purpose(s) of the disputed processing operations are not set out sufficiently

clear and consistent in the standards invoked

107. As mentioned above, under Article 6.3 of the GDPR, the processing referred to in

points (c) and (e) of paragraph 1 must be provided for by Union law or the law of a State

46 See the first respondent's data protection impact assessment, Exhibit 29, under the "DPIA" tab.

Free translation: Currently, there is no legal framework. No law requires or authorizes airports to

measure the body temperature of passengers.

47 Free translation: Brussels Airport is based on a Ministerial Decree (AM of 23 March 2020 containing measures

to limit the spread of the coronavirus COVID-19) and on the FAQs of the National Crisis Center and a Protocol

established by the Safety Council for the Belgian aeronautical industry.

member applicable to the controller. Article 6.3 of the GDPR further states that

“the purpose of the processing [is] provided for in this legal basis or, with regard to the

processing referred to in point (e) of paragraph 1 [it is] necessary for the performance of a task

in the public interest or in the exercise of official authority vested in the controller

of treatment”. Recital 45 specifies in relation to the above: It should also

belong to Union law or to the law of a Member State to determine the purpose of the

treatment. In addition, this law could specify the general conditions of this regulation

with which the processing of personal data must comply in order to be lawful,

and establish specifications for the determination of the controller, the type of

personal data processed, the data subjects, the entities to which the

personal data may be disclosed, limitation of purposes, period

storage and other measures to ensure lawful and appropriate processing. the

Union law or the law of a Member State should also determine whether the controller

processing which is entrusted with a mission of public interest or relating to the exercise of

public authority, is a public authority or another person governed by public law ...”48.

108. However,

the Litigation Chamber finds that

standards

invoked by

them

defendants do not state in a clear and unambiguous manner the exact purpose of the

treatment.

109. As for the Ministerial Order of 5 June 2020 and the Law on Civil Security, it should be noted

that neither mentions the disputed processing. It is clear from the terms of

Ministerial Order that the objective of the measures it contains is to "limit the spread

of the coronavirus COVID-19".

110. Similarly, the Commercial Aviation Protocol - which (partially) provides for the processing

disputed - does not contain a clear description of the purposes of the processing mentioned above

above. From the title of the document, we can deduce that the objective of the measures it contains is "the

resumption of activities related to commercial passenger aviation".

The basic terms of the processing have not been established by law

111. As explained above, according to Article 6.3 of the GDPR, read in conjunction with Article 22 of

the Constitution and sections 7 and 8 of the Charter, a legislative norm must establish the

essential characteristics of data processing necessary for the performance of a

mission of public interest or relating to the exercise of the public authority vested in the

48 It is the Litigation Chamber which underlines.

controller. The provisions mentioned above emphasize that the

processing in question must be framed by a sufficiently clear and precise standard, of which

the application is foreseeable for the persons concerned.

112. The Commercial Aviation Protocol, however, does not define the essential elements of the

disputed treatment. This leaves a wide margin of appreciation to those responsible for the

treatment as to how the measurement of body temperature should be carried out.

Consequently, the Protocol even leaves airport managers free to

carry out this control with or without processing personal data and

determine other terms and conditions (such as retention periods) themselves. This

is also demonstrated by the fact that temperature checks have been carried out

differently at the Belgian airports concerned.

The predictability (or unpredictability) of the Commercial Aviation Protocol

113. European case law requires legislation to be foreseeable. Standards

invoked must also be sufficiently accessible to the persons concerned by the

their publication and, in particular, by their nature and their legal consequences for

persons concerned.

114. In this regard, it should be noted that the Protocol does not stipulate the consequences for the

a person who refuses to submit to a temperature check. This item only appears

in the joint EASA and ECDC operational guidelines. The Protocol does not specify

nor the purpose of identification and the principle of two-level control. Furthermore, the

Protocol was not published on time and correctly. It was notably published on the website

website of the Federal Public Service Mobility and Transport after its entry into force.

Insufficient safeguards for the rights and freedoms of data subjects.

115. According to Article 9.2 g) of the GDPR, “appropriate and specific measures [must

be taken] for the safeguard of the fundamental rights and interests of the person

data subject” if the processing of special categories of personal data is

based on the exception contained in the provision mentioned above (i.e. grounds

important in the public interest).

116. As also indicated by the Inspection Service, both the Ministerial Order and the Protocol

enable data controllers to determine the essential terms of the

treatment, such as the choice of technology (cf. the control of the system by the first

defendant with a hard drive with a storage capacity of 1 terabyte) and the periods

conservation (cf.

the five-year retention period set by

the second

defendant).

117. By not reserving the determination of these methods to the legislator, risks derived

important for the rights and freedoms of data subjects appear (for example

the vagueness surrounding the purpose and the complication of the exercise of the rights of individuals

concerned; see also infra title II.6; DPIA). According to the case law of the Court

(Privacy International) cited above, it does not satisfy the condition of taking

appropriate and specific measures to safeguard fundamental rights and

interests of the persons concerned.

118. A third constituent element of Articles 6.1 e) and 9.2 g) of the GDPR is compliance with the

principle of necessity in the context of the disputed processing. In this regard, the Chamber

Litigation recalls that it cannot comment on the medical necessity of this measure

in the context of the fight against COVID-19 as such nor on the accuracy and correctness

opinions and reports quoted. It should be noted, however, that this necessity,

as also mentioned in the investigation report of the Inspection Service, must emerge

the legal basis invoked by the controller (in the present case on the

based on Articles 6.1 e) and 9.2 g) of the GDPR).

119. The defendants argue that the disputed processing was necessary because it

were required by the Commercial Aviation Protocol.

120. However, in this respect, the Litigation Division notes however, as already indicated above,

as the Commercial Aviation Protocol of the Minister of Mobility - both in its version

dated June 11, 2020 than in that dated July 31, 2020 - on page 5 it is indicated what

follows: “The measurement of the body temperature of passengers so that they can travel

with an “immunity passport” is not recommended by EASA and ECDC. EASA

recalls that the relevance of this measure is not supported by the knowledge

current scientists on SARS-CoV-2.49

49 Commercial Aviation Protocol, p. 5. It is the Litigation Chamber which underlines.

Decision on the merits 48/2022 - 34/74

121. The Litigation Division thus notes that

the base

legal

invoked by

them

defendants themselves indicate that the need for the treatment in question was not

established, and therefore concludes that the necessity required by Articles 5.1 c), 6.1 e) and 9.2 g)

has not been sufficiently demonstrated.

In particular, it is noted that this necessity is in no way demonstrated in the present case with regard to

relates to the processing of (special categories of) personal data in

the so-called “second line” control framework. As explained above, questionnaires

forms have been completed by the persons concerned as part of this control of

second line - in addition to carrying out manual temperature control. It emerges from

documents of the file and the hearing that the personal data thus collected are

kept both in paper version and in digital version (more precisely in a file

password-protected Excel global) for a period of 5 years. However, it should

to note first of all that neither the Commercial Aviation Protocol nor the Royal Decree relating to

the granting of exploitation rights, nor the Ministerial Order invoked contain the slightest reason

justifying this treatment. The defendants base this processing solely on the

EASA guidelines. As regards the retention period of five years applied, it

It appears from the documents in the file that the defendants refer in this respect to the Law relating to

the rights of patients50 and the obligation to keep the medical records it contains. The

second defendant indicates in this respect that “it was decided to provide for a period of

retention of 5 years, period motivated by the possibility for the passenger to initiate an action in

liability against [the second defendant] (5 years being the limitation period for a

non-contractual action)”. It is apparent from the foregoing that the methods of processing have

been determined by the defendants themselves and not by the legal standards

invoked, as required by Article 6.3 of the GDPR, read in conjunction with Articles 7 and 8 of

the Charter of Fundamental Rights of the EU and 22 of the Constitution.

122. For the reasons set out above, the Litigation Division finds that there has been

the case infringes Articles 5.1 c), 6.1 e), 6.3 and 9.2 g) of the GDPR. The infractions

mentioned above are attributable to both the first and the second defendants,

given that, as explained above, the first defendant must be considered

as controller for the processing of personal data

as part of first-line control and both should be considered as

joint controllers for personal data in the context of

second line control.

50 The law of 22 August 2002 on patients' rights, M.B. 26 September 2002.

123. The Litigation Division understands the urgency with which the measures were taken in

in the fight against the COVID-19 pandemic. However, it recalls that this does not affect

not the fact that the requirements of the aforementioned provisions, which constitute protection

essential of the rights and freedoms within the framework of the right to the protection of personal data

personal, must be respected.

124. The defendants, as controllers of the disputed processing operations, are liable, in

pursuant to the liability provided for in Article 5.2 of the GDPR in conjunction with Article 24 of the GDPR, of the

compliance with the principles relating to the protection of personal data (in particular

the principles of lawfulness and necessity and the principle of minimum data processing) and

providing evidence in this regard. The Litigation Chamber recalls in this regard that the
first defendant itself, in the context of its DPIA, established the absence of a basis
legal valid.
125. The Litigation Chamber recalls that, as soon as
start of treatment
litigious,
them
defendants had to ensure that they had a valid reason for lawfulness and exception to the
meaning of Articles 6.1 and 9.2 of the GDPR, respectively. It appears from the DPIA drawn up by the
first defendant that it was indeed aware of the absence of a legal basis
valid for the disputed processing. Analysis of the documents in the file shows that the database
invoked was determined by the defendants only post factum - during the
procedure before the Data Protection Authority. This is also apparent from the absence
any specific reference to the relevant legal basis in the privacy notice of the
first defendant (see below).
126. Furthermore, it should be noted that the legal norms invoked by those responsible for the
processing do not contain any obligation and do not create a legal framework for the realization
of a two-line temperature check, the personal data concerning
the health of data subjects collected as part of second-line control
being kept for a period of 5 years.
127. The Litigation Division finds that the second defendant, in its answer, during
the hearing and in its reaction to the sanction form, submits that no violation of the
articles 5, 6 and 9 of the GDPR could not be held against him given that the investigation report
on its part did not contain any findings in this regard. The second defendant makes
argue that, as a result, the charges brought against it under the aforementioned provisions have not
not been clearly and definitively determined when the procedure was opened before

the Litigation Division, which would not be in accordance with the case law of the Court of

markets.51 It should be noted, however, that the investigation report of the Inspection Service

contains clear findings of fact and law in this regard. In this regard, the House

Litigation refers to sections 3.4 and 3.5 of the investigation report, in which the

Inspection service decides, among other things, on the legality of the disputed processing (art. 5.1 c),

6.1 and 9.2 of the GDPR) with regard to the second defendant, inter alia: “The processing

in the case of BAC not having a basis according to Article 6 of the GDPR (see finding 12), B-Art

can hardly rely on this same basis”.52

128. The Litigation Chamber further recalls that in the contracts concluded between the two

parties, the second defendant was designated as sole controller in

with regard to second-line control and that it was therefore held, in accordance with the

responsibility contained in Article 5.2 of the GDPR, to comply with the provisions of the GDPR, in

in particular Articles 5, 6 and 9 of the GDPR, and to provide proof thereof. Furthermore, the second

defendant had ample opportunity to exercise its rights of defense with respect to

relates to the charges mentioned above. The latter has also made use of this

opportunity. Therefore, the above-mentioned argument of the second defendant does not

can be accepted.53

II.5. The obligation of information and transparency (art. 12-14 of the GDPR)

Findings of the Inspection Service

129. In its investigation report, the Inspection Service finds that the first respondent has

violates the information obligation provided for in Articles 12.1 and 13 of the GDPR54.

130. More specifically, the Inspection Service finds breaches of the aforementioned provisions

regarding the privacy policy, signage in buildings and the

rules of procedure of the first defendant.

131. With regard to the first defendant's declaration of confidentiality, as

published on the website https://www.brusselsairport.be/fr/mentions-legales/privacy-policy

the inspection service finds that it does not contain/did not contain (on the dates of the

verification, i.e. June 14 and October 6, 2020) all information listed in

51 More specifically: Brussels Market Court, February 24, 2021 (2020/AR/1159).

52 Investigation report, p. 38.

53 Cf. reply of the second defendant, p. 9-21.

54 Investigation report point 3.7, p. 38-43.

the aforementioned provisions In particular, the Inspection Service notes in its report that the

following information was not mentioned in a clear or consistent manner:

-

the retention period of personal data (Art. 13.2 a)

GDPR;

-

the identity of the data controller (Art. 13.1 a) of the GDPR; the service

inspection finds in particular that the name and contact details of the

first defendant as such were included in the declaration of

confidentiality, but that they were not sufficiently bound

clear to the disputed processing of personal data;

-

-

the purpose of the processing (Art. 13.1 c) of the GDPR.

the possibility of lodging a complaint with the Data Protection Authority

data (or any other supervisory authority) (Art. 13.2 d) GDPR.

-

the consequences for the data subject (Art. 13.2 e) of the GDPR) if the

data is not provided.

132. With regard to signage in the buildings and the internal regulations of the first

respondent, the Inspection Service finds that:

-

the first defendant infringes article 5.1 a) of the GDPR since the

information relating to the “independent experts” appearing in the

rules of procedure are presented incorrectly or, at all

less, misleading, given that these experts supposedly

self-employed are the subcontractor under contract remunerated by the first

defendant and are bound by the basic contract to the latter;

-

the information that the data is not stored and

retained are incorrect;

-

the first defendant communicates differently with regard to the APD

only with regard to the passengers concerned, since the legal basis is not

clearly communicated to the persons concerned and that it is

only stated “Your health and safety is important to

us", whereas this information falls under the information obligation of

Article 13.2 e) of the GDPR.

133. In addition, the Inspection Service finds that the contacts between the first defendant and

airlines to inform passengers as well as press articles do not

are irrelevant in assessing the duty to inform, since the first defendant cannot

not demonstrate having satisfied its obligation to inform by referring to press releases

of third parties.

Defenses of the first defendant

134. In its response, the first defendant disputes all of the above findings.

135. More specifically, the first defendant argues that:

-

the fact that the second defendant is remunerated for a service that she

performs for the first defendant does not mean that the personnel

(medical) of the first defendant would not work in a manner

independent;

-

no erroneous information has been provided regarding storage

personal data (during first-line control),

since the hard disk with a storage capacity of 1 terabyte

ordered from X has never been used and that, with regard to the

storage of personal data in the second line, the

first defendant did not

never given a mandate to

the second

defendant to store the questionnaires (in filing cabinets

rings);

-

the Privacy Policy contained, in accordance with Article 13.2 a) of the

GDPR, the necessary information regarding the retention period

data and, in particular, that the personal data of

data subjects would not be kept for longer than

necessary for the purpose(s) for which it was collected;

-

the identity of the controller was

clearly indicated

(“Brussels Airport Company SA (hereinafter: “Brussels Airport” or “we”)

and that the Privacy Policy also linked to the

disputed treatment, namely temperature control;

-

the purposes of the processing mentioned in the privacy policy

and in the signage are not contradictory (“your health and your

security” and “missions of public interest”), because both refer to the

mission of public interest - namely ensuring security at the airport - which is

charged the first defendant. The first defendant makes

furthermore, in response to

the observation of the Inspection Service

regarding the length of the privacy policy, than shortening it

would mean that all the necessary information could not be there.

figure;

-

the consequences for the data subject in the event of refusal to provide

the data was only actually mentioned in the regulations

of internal order, but that the GDPR does not require that the mentions

mandatory are provided in a single document;

Decision on the merits 48/2022 - 39/74

-

Following the inspection investigation, changes were made to

the privacy policy, which has been developed in three layers.

Analysis of the Litigation Chamber

136. The Litigation Chamber recalls that, in accordance with Article 12.1 of the GDPR, the controller “[shall take] appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under of Articles 15 to 22 and Article 34 with regard to the processing to the data subject in a concise, transparent, understandable and easily accessible manner, in terms clear and simple (...)”.

137. Recitals 58 and 60 of the GDPR specify that “The principle of fair and transparent requires that the person concerned be informed of the existence of the operation of processing and its purposes" and that "the principle of transparency requires that any information addressed to the public or to the person concerned is concise, easily accessible and easy to understand, and formulated in clear and simple terms (...)”.

138. In the event that the personal data concerned have been collected from the the data subject himself, Article 13 of the GDPR specifies which information must be provided to the latter:

“Where personal data relating to a data subject is collected from this person, the data controller provides him, at the time where the data in question is obtained, all of the following information:

a) the identity and contact details of the controller and, where applicable, of the representative of the controller;

b) where applicable, the contact details of the data protection officer;

c) the purposes of the processing for which the personal data are intended as well as the legal basis of the processing;

d) where the processing is based on Article 6, paragraph 1, point f), the interests legitimate claims pursued by the controller or by a third party; e) recipients or the categories of recipients of the personal data, if they exist;

f) where applicable, the fact that the controller intends to carry out a

transfer of personal data to a third country or to an organization

international community, and the existence or absence of an adequacy decision issued by the

Commission or, in the case of transfers referred to in Article 46 or 47, or Article 49,

paragraph 1, second subparagraph, the reference to the appropriate or suitable safeguards and the

means of obtaining a copy or where they have been made available;

Decision on the merits 48/2022 - 40/74

2. In addition to the information referred to in paragraph 1, the controller shall provide the

the data subject, at the time the personal data is obtained,

the following additional information which is necessary to guarantee a

fair and transparent treatment:

a) the retention period of the personal data or, where this is not

possible, the criteria used to determine this duration;

b) the existence of the right to request from the data controller access to the data to be

personal nature, the rectification or erasure of these, or a limitation of the

processing relating to the data subject, or the right to oppose the processing and

right to data portability;

c) where the processing is based on point (a) of Article 6(1) or on Article 9,

paragraph 2(a), the existence of the right to withdraw consent at any time,

without affecting the lawfulness of the processing based on the consent made before the

withdrawal thereof;

(e) information on whether the requirement to provide data to

personal nature has a regulatory or contractual nature or if it conditions the

conclusion of a contract and whether the data subject is obliged to provide the data to

personal character, as well as on the possible consequences of the non-provision of

those data ;

f) the existence of automated decision-making, including profiling, referred to in

Article 22, paragraphs 1 and 4, and, at least in such cases, useful information

regarding the underlying logic, as well as the significance and intended consequences

of this processing for the data subject.

139. In its transparency guidelines, Working Party 29 clarified that

Article 13 of the GDPR applies both in cases where personal data is

knowingly transmitted by the person concerned to the person responsible for the

processing and in cases where the data is collected by the controller

by observation (e.g. using automated data collection equipment)

data or software for data collection such as cameras).55

140. As regards the declaration of confidentiality of the first defendant (at the time

findings of the Inspection Service), the Litigation Chamber notes that, with regard to

of the retention period of the personal data collected, it did not contain

indeed no concrete period during which the data concerned was

preserved. This stipulates in particular: "We will not keep your data

55 Working Group 29, Guidelines on transparency under Regulation 2016/679, 11 April 2018, p. 14-15, marg. 26.

personal character longer than necessary for the purpose(s) for which

they have been collected or for which they will be processed (...). “However, the Chamber

Litigation recalls that Article 13.2 e) of the GDPR indicates in this respect that the person responsible for the

processing must mention “the retention period of the personal data or,

where this is not possible, the criteria used to determine this duration”. Bedroom

Litigation also finds on the basis of the conclusions of the first defendant

and attachments (see exhibit 34) that it amended this point following the comments of the

Inspection service. The first defendant's privacy policy mentions

now more concrete information regarding retention periods (for

example, 30 days for camera images).

141. With regard to the communication of the identity of the data controller in the

privacy policy of the first defendant, the Chambre

Litigation finds no violation. It appears from the documents in the file that the latter

contained (also at the time of the findings) a sufficiently clear reference to the

legal entity “Brussels Airport Company SA” as data controller

data collected and processed: “Brussels Airport Company SA” (hereinafter: “Brussels

Airport" or "we") respects your privacy and protects and processes your Personal Data

personnel in accordance with the General Data Protection Regulation (...). " It was

also sufficiently clear with regard to the processing activity concerned (the

temperature control): “Temperature control. Departing and arriving passengers

must go through a temperature check. Brussels Airport does not keep the

data resulting from these measurements and does not transmit them to unauthorized third parties (...). »

142. With regard to the purposes of the processing, the Inspection Service notes that the

information mentioned on the airport signage does not correspond to the

information contained in the privacy policy of the first defendant. This

especially since the signage did not expressly mention the purposes and the basis

legal basis for the disputed processing, in accordance with Article 13.1 c) of the GDPR (“the purposes of the

processing for which the personal data are intended as well as the basis

legal basis of the processing”). In this regard, the Litigation Chamber finds, on the basis of the

response from the first defendant as well as the documents in the file, that the indication

did refer to the privacy policy of the first defendant on the site

internet of it. The Litigation Chamber concludes that the obligation of Article 13.1 c) of the

GDPR is fulfilled.

143. With regard to the mention of the possibility of lodging a complaint with

the data protection authority (Art. 13.2 d) of the GDPR), the Inspection Service finds

that “the person concerned [must consult] a separate online document of 25 pages (the

privacy policy) to learn that they can lodge a complaint with

ODA, which is not so obvious if one is in a hurry on the way to or from a

destination ". The Litigation Chamber finds that

the possibility of introducing a

complaint to the APD was not actually mentioned on the signage, but

that it did appear in the confidentiality policy of the first defendant, to which

the signaling refers: "In addition, you can also lodge a complaint

with the Data Protection Authority, which you can contact by e-mail:

contact@apd-gba.be”. The Litigation Chamber considers that the first defendant has

thus fulfills the requirement of Article 13.2 d) of the GDPR. With regard to the point mentioned

above, the Litigation Division only notes that, in accordance with the provision

mentioned above, the parties concerned not only have the right to lodge a complaint

with the Belgian DPA, but also with any other European supervisory authority. He

is therefore appropriate - especially given the international audience in the case

present - to also specify this in the privacy policy.

144. With regard to the consequences for the data subject if the data is not

provided (Art. 13.2 e) of the GDPR), the Inspection Service finds that this information is not

not clear in privacy policy or signage. It indicates in particular

that the person concerned must consult several documents to obtain the information

required. It is apparent from the response of the first defendant and from the documents in the file that

them

information mentioned above did not actually appear in

the declaration of

confidentiality and were only mentioned in the rules of procedure of the first

defendant and on signage. The rules of procedure state the following in this regard:

“In the case of a departing passenger, the passenger will be referred to medical experts

independent who will assess whether the passenger presents a risk and whether access to the airport should

therefore be denied him. Persons entering the airport on arriving flights will be

Please leave the building as soon as possible. » The Litigation Chamber is

of the opinion that, in accordance with Article 12 of the GDPR combined with Article 13.2 e) of the GDPR, the

first defendant should have included the information mentioned above in its

privacy policy in order to make them available to data subjects under

“an easily accessible form”.

145. The Litigation Chamber also notes - like the Inspection Service - according to the

documents in the file, that the privacy policy does not clearly indicate the legal basis

used, as required by Article 13.2 e) of the GDPR. The privacy policy is one

general mention of “legal obligations and missions of public interest”, but does not specify

not which of the two (art. 6.1 c) or 6.1 e) of the GDPR) is applicable to the disputed processing. the

Decision on the merits 48/2022 - 43/74

text also does not mention the standards which were then indicated by the first

defendant during the proceedings before the Litigation Chamber as a basis

of the disputed processing, within the meaning of Articles 6.1 e) combined with Art. 6.3 GDPR and

9.2 g) of the GDPR (i.e. the Royal Decree granting the operating license, the Ministerial Order of 5 June

2020 on urgent measures to limit the spread of the coronavirus COVID-19,

the law of December 31, 1963 on civil protection [as replaced by the law of

May 15, 2007] and the Commercial Aviation Protocol of June 11, 2020).

146. Point 4.6.1 of the privacy policy as published on October 6, 2020

only indicates the following:

“4.6.1 Statutory obligations and public interest missions

(…)

Temperature screening Departing and arriving passengers must pass through a

temperature control. Brussels Airport does not keep the data of these measures

and does not pass them on to unauthorized third parties. The medical checks that can

possibly follow are carried out by doctors. »

147. The Litigation Division draws attention to the essential nature of this information, which

relates to the lawfulness of the disputed processing within the meaning of Articles 6 and 9 of the GDPR, and emphasizes that

the ground of lawfulness and the legal bases they contain must be established no later than

start of the processing of personal data, and be communicated in a manner

transparent to the people concerned. It can no longer be determined a posteriori.

As Advocate General P. Cruz Villalón and the Court of Justice of the European Union pointed out

European Union in the Bara case56, compliance with the provisions on transparency and

information is essential, as it constitutes a precondition for the exercise by the

data subjects of their rights, which are one of the foundations of the GDPR. Bedroom

Contentious emphasizes, as already mentioned above (see above n° 125 and 145), that it is not

therefore in no way acceptable that the legal basis of the processing is determined or

specified by the controller only during the DPA procedure.

148. Based on the foregoing, the Litigation Chamber finds that the first

defendant has breached Article 12 in conjunction with Articles 13.1 c) and 13.2 e) of the

GDPR.

149. With regard to the confidentiality statement of the second respondent, the Chamber

Litigation finds that

the version as it is published on

the site

Internet

56 EU CdJ, 1 October 2015, Bara, C-201/14, point 33 (Principles of Advocate General P. Cruz Villalón, 9 July 2015, para.

74).

https://www.ambuce.be/privacy-policy/ at the start of the investigation by the Inspection Service

did not contain any information concerning the disputed processing of the personal data

personal.

150. As noted by the Inspection Service in its investigation report, the second

defendant published a new privacy statement on its website after

the beginning of this investigation https://www.ambuce.be/airport-rescue/.

151. In its investigation report, the Inspection Service indicates that, given the importance

of an effective and proportionate investigation, no further investigation has been carried out into

the comparison of the consistency of the privacy policies of the first and the

second defendant. This taking into account the qualification by the Inspection Service of

the latter as a subcontractor.57

152. The Litigation Division recalls that the second defendant was also required to

comply with the transparency obligations imposed by articles 12 and following of the GDPR. He

should be noted in this respect that the contracts concluded between the first and the second

defendant qualified the latter as controller and that it therefore had to

act accordingly with regard to the transparency obligations imposed on

GDPR controllers.

153. Since this aspect has not been investigated in depth by the Inspection Service, no offense can be

however, be found against the second defendant in this respect.

II.6. Impact analysis relating to data protection (article 35 of the GDPR)

Findings of the Inspection Service

154. In its investigation report, the Inspection Service notes several violations concerning

the data protection impact assessment (DPIA) carried out by the first

defendant:

- First of all, the Inspection Service notes that this DPIA does not contain

not all the information required by article 35.7 of the GDPR.

- Second,

the Inspection Service argues that

the first one

defendant did not sufficiently take into account the context of the

processing in the DPIA. In this regard, the Inspection Service indicates more

57 See the Inspection Service investigation report, p. 44.

precisely that the DPIA was not used as an instrument

to reassess the risks and effectiveness of the disputed treatment.

- Third,

the inspection service

stated in his report

of investigation that the first defendant denies its responsibility for a

part of the processing and has excluded that part from the scope of

the DPIA.

- Fourth,

the Inspection Service finds that

the first one

defendant did not apply the three elements contained in Article

24.1 of the GDPR, namely (i) taking into account the context, (ii) taking

organizational measures and (iii) evaluate and update the measures

technical and organizational.

- Fifth,

the inspection service

stated in his report

survey that the risk depending on the type of treatment, in particular the

processing of health-related data, has been insufficiently examined.

- Sixthly, the Inspection Service argues that the DPIA does not contain

proper investigation of the standards invoked.

- Seventhly, the Inspection Service indicates that the DPIA contains a

methodological flaw that prevents it from examining the risks for

rights and freedoms of natural persons.

- Eighth, the Inspection Service asserts that the DPIA contains

inaccurate statements or an understatement of the facts.

- Ninthly, the Inspection Service notes in its investigation report

that the DPIA has not been subject to external review.

Defenses of the first defendant

155. The first defendant submits that neither the GDPR nor the DPA imposes or proposes a

template for the development of a data protection impact assessment.

156. With regard to the findings of the Inspection Service, the first respondent

argue that:

-

it contains all the information prescribed by article 35.7 of the

GDPR. In its answer, the first defendant includes in this regard a

summary table of all the requirements as well as mentions.

-

the context of the processing was sufficiently exposed and that it was not

necessary to update the DPIA since no modification had been

made to the temperature control process since June 2020.

-

it has not included inaccurate declarations in the DPIA.

Defenses of the second defendant

157. With regard to the findings of the Inspection Service concerning the DPIA, the second

defendant declares that:

-

it cannot comment on the DPIA carried out by the first

defendant.

-

it considers that carrying out a DPIA was not necessary for the

second-line control since the data processing in question does not

did not fall under Article 35 of the GDPR. In this regard, the second defendant

argues in the first place that the processing of data relating to health

as part of the second line of control was not carried out to a large extent

scale and refers, in this respect, to recital 91 of the GDPR. She specifies

that an average of eight passengers were subject to this check. Secondly

place, the second defendant argues that the disputed processing does not

does not fall under any of the cases in the list of processing operations for which, according to

the Data Protection Authority, a DPIA must be carried out

in accordance with Article 35.4 of the GDPR.

-

the fact that no DPIA has been carried out with regard to the control

second-line does not mean that no (risk) analysis would have had

place in this regard. In this regard, it specifies that the processes relating to the

processing of the disputed data have been carefully worked out in

prior, assessed and - if necessary - adapted.

Analysis of the Litigation Chamber

General

158. Article 35 of the GDPR lists the cases in which the execution of a DPIA is required. In

particular, the aforementioned provision indicates that “when a type of processing, in particular by

the use of new technologies, and taking into account the nature, scope, context

and the purposes of the processing, is likely to create a high risk for the rights and

freedoms of natural persons, the controller performs, before the processing,

an analysis of the impact of the planned processing operations on the protection of

personal data”.58

58 Article 35.1 of the GDPR.

159. Article 35.3 of the GDPR provides that a DPIA is required in particular in the following cases:

has)

the systematic and in-depth assessment of personal aspects concerning

natural persons, which is based on automated processing, including profiling,

and on the basis of which decisions are taken which produce legal effects for

with respect to a natural person or significantly affecting him in a similar way;

b)

large-scale processing of special categories of data referred to in Article 9,

paragraph 1, or personal data relating to convictions

criminal offenses and offenses referred to in Article 10; Where

vs)

systematic large-scale monitoring of an area accessible to the public.

160. In accordance with Article 35.4 of the GDPR, the Data Protection Authority has also

published on its website a list of the types of processing for which an analysis

impact on data protection is also mandatory.59 According to the list

mentioned above, the completion of a DPIA is also required in the following cases

notably :

1)

when the processing uses biometric data for unique identification

data subjects in a public place or in an accessible private place

to the public ;

2)

when data is collected on a large scale from third parties in order to analyze or

to predict the economic situation, health, preferences or centers of interest

personal data, the reliability or the behavior, location or movements of

physical persons ;

3)

when the health data of a data subject are collected through

automated using an active implantable medical device;

4)

when data is collected on a large scale from third parties in order to analyze or

to predict the economic situation, health, preferences or centers of interest

personal data, the reliability or the behavior, location or movements of

physical persons ;

5)

when special categories of personal data within the meaning of Article

9 GDPR or data of a very personal nature (such as data on the

poverty, unemployment, involvement of youth aid or social work, data

on domestic and private activities, location data) are exchanged

systematically between several data controllers;

6)

when it comes to large-scale processing of data generated by means of

devices with sensors that send data over the internet or through another

Medium (“Internet of Things” applications, such as smart TVs,

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

Decision on the merits 48/2022 - 48/74

smart household appliances, connected toys, “smart cities”, meters

intelligent energy systems, etc.) and that this processing is used to analyze or predict the situation

economic, health, personal preferences or interests, reliability or

behaviour, location or movements of natural persons;

7)

when it comes to large-scale and/or systematic processing of personal data

telephony, internet or other communication data, metadata or

location data of natural persons or allowing to lead to

natural persons (for example wifi tracking or data processing of

location of travelers in public transport) when the processing is not

strictly necessary for a service requested by the data subject;

8)

when it comes to processing personal data on a large scale

where the behavior of natural persons is observed, collected, established or influenced, including

including for advertising purposes, and this systematically via processing

automated.

161. With regard to the use of thermal cameras, the Litigation Chamber recalls that

the European Data Protection Supervisor (EDPS) has already confirmed

explicitly in a position paper dated February 1, 2016 that the achievement of a

AIPD is required in this respect.60 Consequently, the Litigation Chamber considers that a

AIPD should actually be carried out for the processing of personal data

personnel as part of first-line control, through the use of thermal cameras.

162. The Litigation Division emphasizes that the need to carry out a DPIA in this case is

also confirmed by recital 91 of the GDPR which states: that “an impact assessment

relating to data protection should also be carried out when data to be

personal nature are processed for the purpose of making decisions relating to persons

specific physical features following a systematic and in-depth evaluation of aspects

personal data specific to natural persons on the basis of the profiling of said data or

as a result of the processing of special categories of personal data,

biometric data or data relating to criminal convictions and

offences, or related security measures”.

163. It is common ground in the present case that the processing in question relates to specific categories

of data (health data) and that, at least with regard to the

processing during a departure, it has the effect of deciding whether or not passengers can enter

in the airport terminal.

60 https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/use-thermal-imaging-cameras-

and-auto_en.

164. The Litigation Division does not rule in this case on the question of whether the

thermal imaging cameras used should be considered “new technology”

within the meaning of Article 35.1 of the GDPR, but points out that in the present case this cannot

lead to a different conclusion since, in accordance with what has been explained above,

a DPIA was necessary in this case.

165. The Litigation Division assesses below the various findings of the Service

inspection with regard to the DPIA, in the light of the defenses of the two

defendants.

Finding 1: concerning the obligation to carry out a DPIA before the start of treatment and

to take into account the context of the processing in the DPIA (art. 35.1 of the GDPR)

166. According to Article 35.1 of the GDPR and recital 90 of the GDPR, the controller must

first carry out the DPIA before the start of the processing of personal data

concerned.

167. The Inspection Service's investigation report and the documents in the file show that the

first defendant began to carry out the DPIA on June 5, 2020 and that it ended

completed on June 25, 2020. The relevant processing started on June 15, 2020. The first

defendant asserts in this regard in its letter dated November 15, 2020 addressed to the

Inspection service: "For the launch of the temperature control, the AIPD was drawn up,

in terms of content, with the departments concerned at [the first defendant],

as shown in the email of June 11, 2020 (Annex 1). The final signature (official signature) has

took place on June 25, 2020 (Annex 2). It should be taken into account that this project was launched within

from the airport in a very short time. The protocol describing the temperature control has not

was brought to the attention of [the first defendant] only on June 11, 2020".61

168. The Inspection Service also notes in this respect that it appears from the documents in the file and

the chronology that the first defendant only decided to carry out a DPIA after having

decided to place an order with X and the second defendant in connection with the treatment

contentious.62

61 Exhibit 30 Inspection Service file, p. 5.

62 Investigation report, p. 46-47.

169. Based on the foregoing, the Litigation Division considers that the requirement to carry out

the DPIA before the start of the processing of personal data has not been complied with,

since the DPIA was not finalized until after the start of the disputed processing. Therefore, the

Litigation Chamber considers that there is reason to note a violation of Article 35.1 of the

GDPR on the part of the first defendant for not having completed the DPIA before the

start of the disputed treatment.

170. Article 35.1 (combined with Article 24 of the GDPR) secondly provides that the data controller

processing, when carrying out the DPIA, must take into account “the nature, scope,
context and purposes of the processing” in order to assess the risk.
171. In its investigation report, the Inspection Service notes in this respect that the first
defendant did not sufficiently take into account the changing context when
achievement of the DPIA and did not sufficiently use the DPIA as a tool for reassessing the
disputed treatment.
172. In this regard, the first respondent states in its response that it considers that it has
sufficiently describes the processing in the DPIA. This indicates that during the period of
temperature control, there was no need to update the DPIA because, since June 2020,
there were no changes in the temperature control process that would have
changed the risks and that the need for temperature control remained unchanged in
the lack of more appropriate alternatives to detect COVID-19 at the airport.
173. With regard to this second aspect, the Litigation Chamber underlines that the realization
of a DPIA should in fact not be seen as a one-off exercise, but rather
as a continuous exercise, and that - in the context of responsibility - it is good
practice to regularly review and reassess a DPIA. In this regard, it should be
refer to article 35.11 of the GDPR and to the Guidelines on Data Protection Impact Assessment
(DPIA) and determining whether processing is “likely to result in a high risk” for the purposes
of Regulation 2016/679 of 4 April 2017, according to which a review of the DPIA is appropriate in
case of “modification of the risk presented by processing operations”.63
174. However, with regard to this second aspect, the Litigation Chamber notes that in
case, it cannot be established that, between the time the DPIA was carried out in June 2020 and
discontinuation of the disputed treatment in January 2021, there was a change in the risk associated with
63 See GDPR Article 35.11 in fine and Working Group 29, Guidelines on Data Protection Impact Assessment (DPIA) and
determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 4 April 2017, p.
12.

aforementioned processing which required a revision of the DPIA. No offense is therefore
observed in this regard.

Findings 2 and 3: with regard to the limitation of processing in the DPIA (Art. 35.7 of the
GDPR) and keeping part of the processing out of scope

175. In accordance with Article 35.7 of the GDPR, the DPIA must contain at least the information
following:

has. a systematic description of the processing operations envisaged and the purposes of the
processing, including, where applicable, the legitimate interest pursued by the data controller
treatment ;

b. an assessment of the necessity and proportionality of the processing operations
regard to the purposes;

vs. an assessment of the risks to the rights and freedoms of data subjects
in accordance with paragraph 1; and

d.

the measures envisaged to deal with the risks, including guarantees, measures and
security mechanisms to ensure the protection of personal data
and to provide proof of compliance with these regulations, taking into account the rights and
legitimate interests of data subjects and other affected persons.

176. According to the findings of the Inspection Service in the investigation report, no
sufficiently fulfills the obligation to describe and delimit the disputed processing (Art. 35.7
a) GDPR). In this regard, the Inspection Service indicates that the first and second checks
second line are not explicitly mentioned, nor is the reason for the processing.64

177. It appears from the documents in the file that the DPIA describes the disputed processing in the tabs
entitled “Identify the needs”, “Information flows” and “DPIA” of the document sent by the
first defendant. In this regard, the first tab mentions: “Project Name:

Temperature Screening COVID19”.

64 Investigation report, p. 49.

178. The “Information flow” tab mentions: “Processor: X gets a notification as soon as a passenger passed. X does not in any way process personal data for other use then sending passenger on to additional check if required. They only register the number of passengers going through the check. Also medical checks are done by medical staff and neither BAC or X are involved. »65

179. The “DPIA” tab contains additional descriptions, such as “In case of high temperature the passenger is assisted towards medical staff that decides if a person is allowed to continue his trip. Medical staff will perform an elaborate medical check by doing a manual temperature check as well as other medical tests and an interview. »66

180. With regard to the purposes of the processing, it is noted that the “DPIA” tab, under the assessment of the risks to the rights and freedoms of the persons concerned, indicates: “(...) purpose: detecting potential COVID19 cases”.

181. On the basis of the foregoing, the Litigation Division finds that the information required by Article 35.1 a) of the GDPR are not included centrally in the DPIA, which does not does not promote readability. It should be noted, however, that Article 35 of the GDPR does not impose no particular form requirement in this respect and contains only the particulars mandatory. The Litigation Chamber therefore finds no breach of Article 35.7 of the GDPR in this regard.

182. However, the Litigation Division notes, like the Inspection Service in its investigation report67, that the DPIA only relates to first-line control (control of the

65 Free translation: “Subcontractor: X receives a notification when a passenger has passed. X does not in any case process the personal data for purposes other than directing the passenger to further screening if necessary. It only records the number of passengers passing through the checkpoint. Medical checks are

also performed by medical personnel, but neither BAC nor X are involved. »

66Free translation: “In case of high temperature, the passenger is accompanied to the medical personnel

who decides whether the person can continue their journey. The medical staff carry out an extensive medical check-up by mean

a manual temperature check and other medical tests, as well as an interview.”

67 Investigation report, p. 49-50.

temperature) and does not contain a risk assessment regarding second-hand control

line.

183. With regard to the question of whether or not to carry out a DPIA with regard to

concerns the control of the second line, the first and second defendants indicate

in their conclusions in response that there has been no processing of personal data

large-scale personnel within the meaning of Article 35 of the GDPR and refer to recital 91 of the

GDPR, according to which the processing of personal data should not be considered

as processing on a large scale when it comes to the processing of personal data

patient or client staff by an individual physician, other healthcare professional

health or a lawyer. According to the defendants, the processing carried out in the context of the

second-line control is therefore comparable to the processing of personal data

staffing of patients by an individual doctor and therefore a DPIA could not

be required for the processing carried out in this context. The first defendant makes

further arguing that there are two separate data controllers and that it was not

responsible for second line control. She was therefore not required to prepare a DPIA

for these processing operations.

184. The Litigation Chamber recalls that the processing of personal data during

of second-line control cannot, however, be considered (exclusively) as a

processing of patient data by an individual physician. In this context, it is appropriate

to recall that the aforementioned recital 91 of the GDPR also indicates that “an analysis

impact assessment relating to data protection should also be carried out when

personal data are processed for the purpose of making decisions about

specific natural persons following a systematic and thorough assessment

personal aspects specific to natural persons on the basis of the profiling of said

data or as a result of the processing of special categories of personal data

personal data, biometric data or data relating to criminal convictions

and offences, or related security measures".68

185. The Litigation Division finds that in the present case, there is indeed a processing of data

personal character (more precisely of special categories of personal data

personnel) on the basis of which a decision was taken with regard to a natural person

determined, namely the decision whether or not to grant access to the airport terminal to the

concerned person. The above argument of the defendants cannot therefore be

accepted.

68 It is the Litigation Chamber which underlines.

186. As to whether or not the processing was on a large scale, the Chamber

Litigation emphasizes first of all that at the time when the DPIA was to be carried out by the

parties, it was unclear what percentage of passengers undergoing temperature screening

would have a body temperature of 38°C or higher and would then be screened by

second line. Therefore, in this case, it had to be considered that all passengers

controlled could potentially be affected by this processing and take into account

this figure to assess the massive nature or not of the treatment.

187. In addition, it should be noted that the massive nature of the processing of categories

particulars of personal data is not solely determined by the

number of people involved. In this regard, the second defendant points out that in

average, only eight people were subjected to the second-line check, so that

the disputed processing does not fall under Article 35.3 b) of the GDPR. Nevertheless,

in accordance with the guidelines of Working Group 29, the massive character (or not) of the

treatment must be assessed on the basis of several factors: (a) the number of people

concerned, (b) the amount of personal data and/or the scope of the data

data subjects, (c) the duration or continuous nature of the processing activity and (d) the scope

geographical area of treatment.69

188. The Litigation Chamber ruled that, consequently, it was necessary to carry out a DPIA which

also included the processing of personal data in the context of the

second line control. In this regard, the Litigation Chamber also agrees with the

finding of the Inspection Service and considers that a breach of Articles 35.1 and 35.3 of the

GDPR was committed by the two defendants due to the absence in the DPIA

an assessment of the risks associated with second-line treatments.

189. The Litigation Division finds that the second defendant, in its response, when

the hearing and in its reaction to the sanction form, submits that no breach of

article 35 of the GDPR could not be used against it since the investigation report does not

would contain no statement in this regard. The second defendant submits that,

fact, the charges brought against it under the aforementioned provision have not been

clearly and definitively determined at the opening of the procedure before the

Litigation Division, which would not be in accordance with the case law of the Court of

markets.70 It should be noted, however, that the investigation report of the Inspection Service

does contain clear findings of fact and law in this regard, indicating, among other things:

69 Working Group 29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is

“likely to result in a high risk” for the purposes of Regulation 2016/679, 4 April 2017, p. 9.

70 More specifically: Brussels Market Court, February 24, 2021 (2020/AR/1159).

“On the other hand, B-Art has confirmed that it has not carried out an impact analysis for this part of the

same treatment, because it considers that “no impact assessment is required”, because this does not
would not fall under Article 35 of the GDPR. The combination of these two elements means that the
the most sensitive and risky treatments are currently completely excluded from
the DPIA (irrespective of who is responsible for the processing), because BAC
denies its responsibility and B-Art even considers that no analysis should take place. »71
190. The Litigation Chamber further recalls that in the contracts concluded between the two
parties, the second defendant was designated as sole controller in
with regard to second-line control and that it was therefore held, in accordance with the
responsibility contained in article 5.2 of the GDPR, to comply with the provisions of the GDPR,
in particular Article 35 of the GDPR, and to provide proof thereof. Furthermore, the second
defendant had ample opportunity to exercise its rights of defense in relation to the
charge mentioned above. The latter has also made use of this opportunity. By
Therefore, the above-mentioned argument of the second defendant cannot be
accepted.72
Finding 4: regarding the examination of the standards invoked
191. In accordance with Article 35.10 of the GDPR, if the processing under Article 6.1 c) or e) of the
GDPR has the legal basis of Union law or the law of a Member State, it is assumed
that a general DPIA is carried out by the normative authority.
192. In this regard, the Inspection Service notes in its investigation report that the normative authority
did not carry out a DPIA.
193. In the DPIA carried out by the first defendant, one of the risks identified for the rights
and freedoms of natural persons is repeated as follows: “currently there is no legal
framework. No law exists that obliges or allows airports to check the temperature of
passengers”.73 The first defendant itself describes the impact of the aforementioned risk as
“critical”. In the initial version of the DPIA sent to the Inspection Service, the first
defendant does not provide a solution to this identified risk. In the DPIA version

submitted to the Litigation Chamber as an appendix to the response, the following is indicated under "risk□

solution": "Brussels Airport bases itself on a Ministerial Decree (AM of 23 March 2020□

containing urgent measures to limit the spread of the coronavirus COVID-19) and□

71 Investigation report, p. 50.□

72 Cf. reply of the second defendant, marg. no. 57-59.□

73 See the first respondent's data protection impact assessment, Exhibit 29, under the "DPIA" tab.□

Free translation: Currently, there is no legal framework. No law requires or authorizes airports to□

measure the body temperature of passengers.□

FAQ of the National Crisis Center and a Protocol drafted by the Security Council for the□

aviation industry in Belgium. 74 However, the DPIA - contrary to the answers presented□

by the first and second defendants - makes no mention of the directives□

of EASA and ECDC.□

194. The DPIA indicates in its latest version that the risk of not having a legal framework□

valid is reduced to 32% (residual risk) by the existence of the Ministerial Order and the Protocol□

mentioned above. However, the absence of a legal basis cannot lead to such a□

conclusion. As indicated in the investigation report drawn up by the Inspection Service, the□

only conclusion regarding this identified risk should be "no tolerance". Indeed, the□

processing cannot take place if there is no valid legal basis.□

195. On the basis of the foregoing, it must be concluded that the DPIA carried out by the first defendant□

does not contain an adequate examination of (the lack of quality of) the standard invoked and, therefore,□

therefore, of the necessity and the obligation of the treatment incumbent upon him. Consequently,□

the Litigation Chamber judges that an infringement of Article 35.7 of the GDPR has been committed.□

II.7. The position of the Data Protection Officer (Articles 37-39 GDPR)□

Findings of the Inspection Service□

196. In its investigation report, the Inspection Service notes that the Protection Officer□

of the data of the first defendant was hindered in its ability to exercise its

functions independently within the meaning of Article 39 of the GDPR. The Inspection Service

argues that it is therefore not demonstrated that Article 37.5 GDPR has been complied with.75

197. The Inspection Service bases this observation in particular on the following elements:

▪

it notes that the data protection officer - at the time of the inspection investigation

- was governed by two “privacy platforms”, namely the “Privacy Committee” and the “Privacy

Watch and Action group”, the Privacy Committee being composed of the Director Compliance &

Operations Continuity, the Director Legal & Regulations, the Chief Experience Officer, the

Head of Compliance & Certification Unit and Data Protection Officer. The service

inspection indicates that the Committee is therefore composed of two superiors of the delegate;

74Free translation: Brussels Airport is based on a Ministerial Decree (AM of 23 March 2020 containing measures

to limit the spread of the coronavirus COVID-19) and on the FAQs of the National Crisis Center and a Protocol

established by the Safety Council for the Belgian aeronautical industry.

75 Investigation report, p. 67.

▪ that, according to the manual, the Privacy Committee is entrusted with some of the tasks that the GDPR

assigns to the delegate. The Inspection Service indicates that the Privacy Committee “ensures

the application of privacy and data protection regulations to

personal nature” whereas, according to Article 39.1 b) of the GDPR, it is the responsibility of the delegate to

ensure compliance with the GDPR, without conflict of interest (article 38.6 of the GDPR).

Defenses of the first defendant

198. The first respondent contests the aforementioned finding of the Inspection Service and

states in its response that76:

- since January 1, 2021, the Data Protection Officer is part of the

“Legal & Regulations” department;

-

the Privacy Committee has no control over the Data Protection Officer and

does not influence its decisions in any way, but has the sole purpose of discussing the

pending cases and possible data protection issues;

-

the PRIMA ("Privacy Management Manual") provides for the possibility for the data protection officer

data protection - in the event of a conflict with the committee - to refer the matter to the CEO. The

first defendant refers in this regard to an audit report prepared by Grant

Thornton (prior to the Inspection Service investigation) in which this matter is

addressed.

- BAC also refers to the new measures introduced as a result of the investigation

inspection77, in particular an adaptation of the PRIMA.

Analysis of the Litigation Chamber

199. In accordance with Article 37.5 of the GDPR, the data protection officer is "designated

on the basis of his professional qualities and, in particular, his knowledge

specialized in data protection law and practice, and its ability

to carry out the tasks referred to in Article 39".

200. In the opinion of the Litigation Division, the documents submitted by the first defendant

to the Inspection Service in response to questions posed by the latter78 demonstrate

sufficiently that the level of training and practical experience of the data protection officer

of the data of the first defendant meet the requirements of the provision

aforementioned. It appears from the letter of December 8, 2020 sent by the first defendant

76 Reply of the first defendant, p. 41-45.

77 Ibid, marg. 69.

78 Exhibits 33 and 34 (letter of December 8, 2020).

to the Inspection Service and its annexes that the person concerned holds a law degree and

an IAPP certificate (CIPP/E and CIPM). The person concerned also has experience

relevant professional. Consequently, the Litigation Division finds no

infringement of Article 37.5 of the GDPR.

201. In accordance with Article 38.3 of the GDPR, the controller ensures that “the

data protection officer does not receive any instructions regarding

the performance of its duties”. Recital 97 of the GDPR adds that “data protection officers

data protection, whether or not they are employees of the controller,

should be able to carry out their functions and missions in full independence”.

202. Article 38.3 of the GDPR further states that “the data protection officer shall

directly report to the highest level of management of the controller or

of the subcontractor". According to the Guidelines for Data Protection Officers

data of the Article 29 Data Protection Working Party of 5 April 2017, such

direct report ensures that

the senior management

(for example

the board

Directors) is aware of the opinions and recommendations of the Data Protection Officer

data as part of its mission to inform and advise the controller

or the subcontractor.79

203. On the basis of the documents transmitted by the first defendant - in particular the Privacy

Management Manual (PRIMA; version of 25/03/2019) - the Litigation Chamber finds

that in

the organization chart,

the delegate to

data protection of

the first one

defendant is under the hierarchical supervision of the Head of Compliance and Certification

Unit, the Director Compliance and Operations Continuity and, finally, the CEO, respectively.

The flowchart also shows a direct dotted line from DPO to DPO.

79 Article 29 Data Protection Working Party, Guidelines for Data Protection Officers,

April 5, 2017, p. 19.

204. Furthermore, it is apparent from the first defendant's PRIMA that its protection officer

data is supervised by two consultation platforms, namely the Privacy Committee

as well as the Privacy Watch and Action Group.

205. With regard to the requirement for a direct report from the data protection officer to the

highest-ranking manager (art. 38.3, in fine GDPR), the Litigation Chamber

finds, on the basis of the documents in the file, that there are no indications leading to the assumption

that in the present case this requirement is not fulfilled. The Litigation Chamber is of the opinion that it

sufficiently appears that a direct line exists between the DPO and the CEO of the data controller.

treatment. This is apparent first of all from the organizational chart presented above ("dotted line"

between the two) as well as PRIMA, in which the job description of CEO indicates that he

"[must] establish and maintain a legal reporting line with the Data Protection Officer

designated data". The audit report produced in early 2020 by Grant Thornton

Bedrijfsrevisoren CV also confirms this ("the DPO function has a legal reporting line to

CEO").

206. Furthermore, with regard to this direct report from the DPO to the CEO, the Litigation Chamber notes

that, following the inspection investigation, the first defendant made efforts to

further strengthen this link between the parties mentioned above, in particular 1) by

drawing up an annual written report by the delegate to the CEO on the main activities of

the past year and 2) by organizing a fortnightly meeting between the DPO and the CEO.

207. With regard to the requirement of independence of the DPO contained in Article 38.3 of the GDPR,

the Litigation Chamber notes that - at the time of the inspection investigation - the relationship with the

data protection officer and his position within the two platforms of

consultation that frames it were not entirely clear. In his investigation report on

this relationship between the DPO and the consultation platforms mentioned above, the

Decision on the merits 48/2022 - 60/74

Inspection Service notes that the former “participates in committees which are entrusted with a

part of a control mission that the GDPR reserves for the delegate, the Committee also placing

his conclusions above those of the delegate and ensuring the follow-up of his “performances””.

208. The Litigation Division recalls that the independence requirement provided for in Article 38.3 of the

GDPR means, according to the Article 29 Working Party Guidelines, that “in

the performance of their duties, data protection officers may not receive

no instructions on how they should deal with a particular matter, e.g.

example on the result to which they must arrive, on the way in which they must investigate

a complaint, or whether or not to consult the supervisory authority. Also, they don't

cannot be instructed to take a particular position on an issue

relating to data protection law, for example a specific interpretation of the

law ". Working Group 29 specifies in this respect that "the autonomous nature of the delegates to

data protection does not [mean] however that they have decision-making powers

other than those required for their duties under Article 39”.

209. In addition, Group 29 states the following in its guidelines:

“If the controller or the processor make decisions that are not

in accordance with the General Data Protection Regulation and the opinion of the Data Protection Officer

data protection, the latter must be given the opportunity to clearly express his opinion

diverge to the most senior line manager and to those who make the decisions. »

210.

It therefore follows from the Guidelines that when assessing the independence of the DPO, one should
take into account two criteria: firstly, this independence must be assessed from
concrete and in situ manner and it must be verified that the DPO has not been subject to any influence or
pressure regarding the way in which he must carry out the tasks entrusted to him in
under the GDPR. In other words, it is the obligation to refrain from any interference in
the tasks of the DPO and the prohibition to impose retaliatory measures on the latter.
Secondly, the GDPR and the guidelines mentioned above contain a
positive obligation according to which the controller must ensure that the DPO can
report its views and work to the highest level of the hierarchy. It's about a
additional form of protection which should enable the Data Protection Officer
data to make their voice heard within the organization. As indicated above, the House
Litigation considers that this last criterion is met.
211. With regard to the first criterion, it appears from the documents in the file that the Privacy Committee
above-mentioned has the particular mission of "[monitoring] the application of the regulations relating to the
privacy and the protection of personal data". In accordance with
Decision on the merits 48/2022 - 61/74
Article 39 of the GDPR, the above is indeed one of the tasks of the Data Protection Officer.
data. It appears from the report of the Inspection Service as well as from the documents transmitted by the
first defendant that two hierarchical superiors of the delegate for the protection of
data (namely the Head of Compliance and Certification Unit and the Director Compliance and
Operations Continuity) sit on the Privacy Committee. Therefore, according to the Inspection Service,
the functions of the data protection officer and those of his superiors are intertwined,
which means de facto that the DPO cannot exercise them completely independently.
212. However, the Litigation Chamber recalls that it cannot be inferred from the sole fact that the DPO
a certain position in the organization chart or in the consultation platforms within
the organization that its independence would be impaired within the meaning of Article 38 of the GDPR. The parts of

file do not concretely indicate that independence would have been compromised in practice

by the circumstances mentioned above.

213. As already mentioned above, the Litigation Chamber nevertheless regrets the lack of

clarity regarding the position of the DPO in relation to consultation platforms, as well as the

confusion created by the formal attribution to the Privacy Committee of tasks referred to in Article 39 of the

GDPR.

214. However, the Litigation Chamber finds, on reading the response of the first

defendant and the attachments, that the latter made a series of changes

formal and practical following the remarks made by the Inspection Service in its

investigation report. In particular, the first defendant shows that several provisions of the

PRIMA on this point have been amended to further ensure the independence of the DPO.

215. The Litigation Chamber finds for the aforementioned reasons that the first defendant did not

does not violate Articles 37 and 38 of the GDPR.

III. Violations noted and penalties

216. Under the terms of Article 100, § 1 of the LCA, the Litigation Chamber has the power to:

1° dismiss the complaint without follow-up;

2° order the dismissal;

3° pronouncing the suspension of the pronouncement;

4° to propose a transaction;

5° issue warnings or reprimands;

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

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

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

9° order compliance of the processing;

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

these to the recipients of the data;

11° order the withdrawal of accreditation from certification bodies;

12° to issue periodic penalty payments;

13° to issue administrative fines;

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

international body;

15° forward the file to the public prosecutor's office in Brussels, which informs it of the

follow-up given to the file;

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

Data protection.

217. As to the administrative fines which may be imposed in accordance with articles 58.2

i) and 83 of the GDPR as well as Articles 100, 13° and 101 of the LCA, Article 83 of the GDPR provides:

"1. Each supervisory authority shall ensure that the administrative fines imposed pursuant to

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

are, in each case, effective, proportionate and dissuasive.

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

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

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

the administrative fine, due account shall be taken, in each case, of the elements

following:

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

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

level of damage they have suffered;

b) whether the breach was committed willfully or negligently;

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

damage suffered by the persons concerned;

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

the technical and organizational measures that they have implemented under the

sections 25 and 32;

e) any relevant breach previously committed by the controller or the

Decision on the merits 48/2022 - 63/74

subcontracting ;

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

to mitigate any negative effects;

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

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

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

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

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

compliance with these measures;

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

certificates approved pursuant to Article 42; and

k) any other aggravating or mitigating circumstance applicable to the circumstances of

the species, such as the financial advantages obtained or the losses avoided, directly or

indirectly, as a result of the violation. »

218. The Litigation Chamber recalls that the administrative fine is not intended to put an end to

an offense committed, but to effectively enforce the provisions of the GDPR.

As is clear from recital 148, the GDPR provides for sanctions, including

administrative fines, for each serious violation - even if it is a first violation

(ascertained) - in addition to or in lieu of the appropriate measures which are imposed by

the supervisory authority.80 The recital mentioned above provides for two cases in which it is

possible to waive a fine, i.e. in case of minor violations or when the fine

would impose a disproportionate burden on a natural person. In the above two cases,

according to recital 148, the fine can be replaced by a warning. The fact that it is

of the first observation of a violation of the GDPR on the part of the controller

in no way prejudices the possibility for the Litigation Chamber to impose a fine

administration. As indicated, the instrument of administrative fines is not intended to

put an end to violations. To this end, the GDPR and the LCA provide for various corrective measures,

including the orders referred to in Article 100, § 1, 8° and 9°, of the LCA.

there

them

understood

sanctions

appropriate

imposed by

80 Recital 148 of the GDPR reads as follows: “In order to strengthen the application of the rules of this Regulation,

of the

of the

administrative fines should be imposed for any violation of this Regulation, in addition to or instead of

of the

measures

regulation.

In the event of a minor violation or if the fine likely to be imposed constitutes a disproportionate burden

for a natural person, a

reminder to

He

however, due consideration should be given to

violation, of

intentional nature of the violation and the measures taken to mitigate the damage suffered, the degree of responsibility

or of

the supervisory authority

became aware of the violation, compliance with the measures ordered against the controller or the

any other aggravating circumstance or

subcontractor, of

mitigating. The application of sanctions including administrative fines should

the object of

appropriate procedural guarantees in accordance with the general principles of Union law and the Charter,

including the right to effective judicial protection and due process. »

any relevant breach previously committed, of

the order can be addressed rather than a fine.

the application of a code of conduct, and

under this

the way in which

gravity and

authorities of

the nature of

control in

the duration of

TO DO

Decision on the merits 48/2022 - 64/74

219. In the present case, the Litigation Division finds the following offences:

As regards the first defendant:

has. articles 5.1 c), 6.1 e) and 9. 2 g) of the GDPR, since the defendant did not indicate,

from the start of the procedure before the DPA (and, a fortiori, from the start of the processing

in dispute), the legal basis on which it was based for the processing and given

that it has not been demonstrated that the disputed processing is necessary for reasons

(important) in the public interest, in accordance with European Union law or

law of a Member State, as required by the aforementioned provisions. Furthermore, the

legal grounds invoked by the defendant (namely the RD

granting the operating license, the Ministerial Order of 5 June 2020 relating to

urgent measures to limit the spread of the COVID-19 coronavirus, the law

of 31 December 1963 relating to civil protection [as replaced by the law

of May 15, 2007] and the Commercial Aviation Protocol of June 11, 2020)

do not meet the requirements of Article 6.1 e) combined with Article 6.3 of the GDPR.

Finally, the standards invoked mentioned above do not provide for the

processing of personal data in the context of the control of

second line - with a retention period of five years. In accordance with

the responsibility stipulated by article 5.2 combined with article 24 of the GDPR, it

responsibility of the data controller(s) to ensure that they have a

valid legal basis before starting the treatment.

b. Article 12 in conjunction with Articles 13.1 c) and 13.2 e) of the GDPR, given that the

privacy policy of Brussels Airport Company NV did not indicate

clearly the legal basis used. The privacy policy is one

general reference to “legal obligations and tasks of general interest”, but

does not specify which of the cases listed in Article 6 of the GDPR (Art. 6.1 c) or 6.1 e)

of the GDPR) was applicable to the disputed processing. The text does not mention

plus the standards that were subsequently indicated during the proceedings before the

Litigation Chamber as being the legal basis of the disputed processing, in the

meaning of articles 6.1 e) taken together with articles 6.3 of the GDPR and 9.2 g) of the GDPR (to

namely the Royal Decree granting the operating license, the Ministerial Order of June 5, 2020

on urgent measures to limit the spread of the coronavirus

COVID-19, the law of 31 December 1963 relating to civil protection [as

replaced by the law of 15 May 2007] and the Commercial Aviation Protocol of

June 11, 2020).

Decision on the merits 48/2022 - 65/74

vs. articles 35.1, 35.3 and 35.7 b) of the GDPR, for having failed to carry out an analysis

impact on the protection of data concerning the risks associated with the processing

personal data in the context of second-line control and

for failing to carry out an adequate examination of the standards invoked and of the

necessity and the resulting processing obligation.

As regards the second defendant:

has. articles 5.1 c), 6.1 e) and 9. 2 g) of the GDPR, given that it has not been demonstrated that the processing

disputed personal data is necessary for (important) reasons

in the public interest under European Union law or the law of a Member State,

as required by the provisions mentioned above. In addition, the legal bases

invoked by the defendant (namely the Royal Decree granting the operating license, the

Ministerial meeting of June 5, 2020 on urgent measures to limit the spread of

coronavirus COVID-19, the law of 31 December 1963 relating to civil protection [as

replaced by the law of May 15, 2007] and the Commercial Aviation Protocol of June 11

2020) do not meet the requirements of Article 6.1 e) combined with Article 6.3 of the GDPR.

Finally, the standards invoked mentioned above do not provide for the

processing of personal data in the context of second-hand control

line - with a retention period of five years. According to responsibility

stipulated by article 5.2 combined with article 24 of the GDPR, it is the responsibility of the controller(s)

of the processing to ensure that they have a valid legal basis before

start treatment.

b. Articles 35.1 and 35.3 of the GDPR, for failing to carry out an impact assessment on the

data protection regarding the risks associated with the processing of personal data

personal character in the context of second-line control.

220. In accordance with article 101 of the LCA, the Litigation Chamber decides to impose a fine

to the First Defendant for breaches of Articles 5.1 c), 6.1 e), 9.2 g), 12

combined with Articles 13.1 c) and 13.2 e), 35.1, 35.3 and 35.7 b) of the GDPR, and to the second defendant

for breaches of Articles 5.1 c), 6.1 e), 9.2 g) GDPR, 35.1 and 35.3 GDPR.

221. In view of Article 83 of the GDPR81, the Litigation Division gives concrete reasons

the imposition of an administrative fine taking into account the following elements:

As regards the first defendant:

has)

the nature, gravity and duration of the infringement (art. 83.2 a) GDPR): the infringements noted

relate in particular to a violation of the provisions of the GDPR relating to the principles of

81 Brussels Court of Appeal (Market Court section), X c. GDPR, Judgment 2020/1471 of February 19, 2020.

data protection (Art. 5 GDPR) and lawfulness of processing (Art. 6 GDPR). A

violation of the provisions mentioned above gives rise to the most severe fines

raised in accordance with Article 83.5 of the GDPR.

The infringements noted also concern a violation of the provisions relating to

the obligations of transparency (art. 12-14 of the GDPR). Compliance with the provisions

mentioned above is essential and must take place at the latest at the start of treatment

personal data. This is in particular to facilitate the exercise of the rights

of the persons concerned.

The processing in terms of the number of data subjects is important. According to

statements made by the first defendant at the hearing, between June 15, 2020 and

January 21, 2021, the number of persons affected was approximately 840,000 with regard to

relates to first-line control (temperature control); 827 people were

subject to second line control.

b)

relevant prior offenses committed by controllers (Art.

83.2 e) of the GDPR): the defendant has never been the subject of coercive proceedings by

the Data Protection Authority.

vs)

the categories of personal data concerned by the infringement (Art. 83.2 g)

of the GDPR): the breaches observed concern specific categories of data

of a personal nature within the meaning of Article 9 of the GDPR, in particular data relating

to the health of the persons concerned. Categories of personal data

mentioned above enjoy special protection under the GDPR.

d) any other aggravating or mitigating circumstance applicable to the circumstances of

case (Art. 83.2 k) of the GDPR): the defendant did not benefit from the

treatment or offences.

As regards the second defendant:

has)

the nature, gravity and duration of the infringement (art. 83.2 a) GDPR): the infringements observed

relate in particular to a violation of the provisions of the GDPR relating to the principles of

data protection (Art. 5 GDPR) and lawfulness of processing (Art. 6 GDPR). A

violation of the provisions mentioned above gives rise to the most severe fines

raised in accordance with Article 83.5 of the GDPR.

The scope of the processing in terms of the number of data subjects is extended.

According

statements made by

the first defendant

during

the audience,

Decision on the merits 48/2022 - 67/74

827 people were subjected to second-line checks between June 15, 2020 and

January 21, 2021.

b)

relevant prior offenses committed by controllers (Art.

83.2 e) of the GDPR): the defendant has never been the subject of coercive proceedings by

the Data Protection Authority.

vs)

the categories of personal data concerned by the infringement (Art. 83.2 g)

of the GDPR): the infringements observed concern specific categories of data

of a personal nature within the meaning of Article 9 of the GDPR, in particular data relating

to the health of the persons concerned. Categories of personal data

mentioned above enjoy special protection under the GDPR.

d) any other aggravating or mitigating circumstance applicable to the circumstances of

case (Art. 83.2 k) of the GDPR): the defendant did not benefit from the

treatment or offences.

222. The elements set out above justify an effective, proportionate and dissuasive sanction,

as referred to in Article 83 of the GDPR.

223. On February 9, 2022, a sanction form ("reaction form against the sanction

contemplated") was sent to the first and second defendants. The two defendants

transmitted

their reaction to

the contents of the form mentioned above

respectively on February 25 and March 2, 2022.

224. The first defendant, in its reaction to the sanction form, states in summary that:

1)

the treatment in question was part of a crisis situation (pandemic of

COVID-19) and that it was imposed by the FPS Mobility and Transport through the Protocol

“Commercial Aviation Passengers”, which was issued on June 11, 2020 to relaunch the

aviation sector;

2)

the assessment of legitimacy and proportionality cannot be made a posteriori;

3)

temperature screening was a very common practice at airports at the time

disputed treatments;

4) it acted in good faith and derived no benefit from the disputed treatment, and that it invested

1,920,004 euros in temperature checks;

5)

the first defendant acted on the basis of the belief that it was solely responsible for the

first line control;

6)

the first defendant has always cooperated fully during the proceedings before

ODA;

7)

the principle of proportionality was respected by the short duration of the treatment as well as by

the short retention period of personal data; and

8) what is proposed is disproportionate to the current financial situation of the

first defendant, of the unintentional nature of the infringement and of the fact that no

alternative was not available. The first defendant claims to have realized a loss of

147 million euros in 2020 and 92 million euros in 2021.

225. The Litigation Division considers that arguments 1 to 3 of the first defendant have already dealt with in point II.3. of this decision.82 With respect to the other arguments, the Litigation Chamber notes that they have already been raised earlier in the proceedings and have already taken into account when determining the administrative fine under Article 83.2 of the GDPR.

226. With regard to the argument raised by the first defendant concerning the nature allegedly disproportionate amount of the administrative fine, the Litigation Chamber recalls that under Article 83.4 of the GDPR, breaches of Articles 12, 13.1 c), 13.2 e), 35.1, 35.3 and 35.7 GDPR are subject to an administrative fine of up to EUR 10,000,000 or 2% of the total annual turnover of the previous financial year. In accordance with article 83.5 of the GDPR, them infringements of articles 5.1, 6.1 and 9.2 of the GDPR are subject to fines administrative costs of up to EUR 20,000,000 or 4% of the total annual turnover of the previous year.

227. The Litigation Chamber bases itself - as provided for in Articles 83.4 and 83.5 of the GDPR - on the annual turnover for the previous financial year (in this case 2020) to determine the amount of the administrative fine. According to the conclusions submitted and the annual accounts filed with the National Bank of Belgium (BNB) by the first defendant, the Litigation Chamber notes that the annual turnover for the 2020 financial year for this the latter amounts to EUR 204,318,091.00.

228. The Litigation Chamber decides to maintain the administrative fine of EUR 200,000 announced in the sanction form. It emphasizes that the aforementioned fine is clearly less than the maximum amounts of 10,000,000 and 20,000,000 euros provided for in Articles 83.4 and 83.5 GDPR. In addition, the fine amounts to only 0.10% of the annual turnover of the company.

first defendant, which is significantly lower than the maximum percentages mentioned

above 2 and 4% provided for in articles 83.4 and 83.5 of the GDPR, which do not have the force of law

only for fines exceeding the aforementioned maximum amounts.

82 In this regard, the Litigation Chamber will send a copy of this decision to the competent minister.

Decision on the merits 48/2022 - 69/74

229. With regard to the first defendant's argument that the administrative fine

in this case is higher than in previous decisions of the Litigation Chamber, it

should be noted that, according to Article 83.2 of the GDPR and the Guidelines of the Working Party

2983, fines are imposed “according to the circumstances of the concrete case”.

230. Furthermore, the Litigation Chamber refers in this regard to the case law of the Court of Appeal of

Brussels, section Cours des Marchés, according to which “the Belgian legal system [does not grant]

value of binding precedent to administrative or judicial decisions. Any decision

of a judge (and this also applies to any decision of an administrative authority, provided

that there is no violation of the principle of equality) is specific and does not extend to any case other than

the one being examined.”84 As regards the amount of the administrative fine imposed, the

Court of Markets also recalled the discretion of the Litigation Chamber:

“This means in practice that the DPA can decide not only not to impose a fine on the

offender, but also that, if it decides to impose a fine, it will be between the

minimum, from 1 EUR, and the maximum provided. The imposed fine is decided by the DPA in

taking into account the criteria listed in Article 83(2) of the GDPR”.85

231. With regard to the last argument of the first defendant concerning the losses it

suffered - which would cause the turnover for 2020 to distort its financial situation - the Chamber

Litigation recalls that it is the turnover which is used as a criterion to calculate the

administrative fines under Article 83 of the GDPR and not the operating result.

232.

The second defendant, in its response to the sanction form, states in summary that:

1) prosecuting and convicting the latter would be contrary to the rights of the defence. More

Specifically, the second defendant argues that the Service's investigation report

inspection does not establish any violation on its part. The

second defendant recalls that it is described as a subcontractor in the report

aforementioned. In addition, it refers to the case law of the Court of Markets and in particular

in its judgment of February 24, 2021, and specifies that it follows from the aforementioned judgment that the party

subject to proceedings must be informed at the start of the proceedings before the

Dispute Chamber, in a complete and definitive manner, of the factual elements and

charges against him;

2) according to the elements included in the reaction form against the sanction envisaged,

she would not be able to formulate an appropriate and substantiated response. The second

83 Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines

for the purposes of Regulation 2016/679, 3 October 2017.

84 Brussels Court of Appeal (Market Court section), SA N.D.P.K. vs. DPA, Judgment 2021/AR/320 of July 7, 2021, p. 12.

85 Ibid., p. 42.

defendant argues that the aforementioned form is too brief and does not allow

to know the precise reasons for the imposition of the sanctions envisaged by the Chamber

Litigation;

3) The proposed fine would be disproportionate to the fact that (1) the processing of

data was considered obvious by the competent Belgian authorities, by

other airports and by the passengers themselves; (2) health protection

public was the only reason for the treatment; (3) she considers herself to be so

sanctioned due to inadequate action and legislative inertia; and (4) none

a complaint has been lodged against the disputed processing by a data subject and

no damage has been suffered by a data subject;

4) The disputed processing activity concerns only a limited part of the turnover

of the second defendant and, consequently, the entire annual turnover does not

may be taken into account to determine the administrative fine.

233. The Litigation Division considers that the second defendant's third argument has

already dealt with in Title II.3 of this Decision.

234. With regard to the second defendant's first argument, the Litigation Chamber

notes first of all that the investigation report of the Inspection Service contains many

findings concerning the infringements with which the second defendant is charged, namely

non-compliance with the principles relating to the processing of personal data and the

lawfulness of the disputed processing, as well as the provisions relating to the DPIA. In this regard, the House

Litigation first refers to sections 3.4 and 3.5 of the investigation report. The service

hereby declares that with regard to the lawfulness of the disputed processing (Art. 5.1

c), 6.1 and 9.2 of the GDPR), inter alia, with regard to the second defendant: “The processing

in the case of BAC not having a basis according to Article 6 of the GDPR (see finding 12), B-Art

can hardly rely on the same basis. »86

In the part of the investigation report concerning the findings relating to the impact assessment

on data protection (section 3.7), the role of the second defendant is also

mentioned (cf. “On the other hand, B-Art has confirmed that it has not carried out an impact analysis for this

part of the same treatment, because it considers that “no impact analysis is required”, because this

would not fall under Article 35 of the GDPR. The combination of these two elements makes the

the most sensitive and risky operations are currently totally excluded from the DPIA

(regardless of who

is responsible for the processing), because BAC denies its responsibility and B-Art even considers that there is

no need to carry out an analysis”87). Consequently, the second defendant cannot

86 Investigation report, p. 38.

87 Investigation report, p. 50.

no case to maintain that the Litigation Chamber added new charges to the procedure,

against which she would not have been able to defend herself.

235. In response to the second respondent's argument regarding the fact that it has been characterized as

subcontractor in the investigation report, the Litigation Chamber recalls that it is not bound

by these findings. On the contrary, it is precisely for the Litigation Chamber

to assess the accuracy of the findings, particularly in the light of the defenses

presented in response to the investigation report. In this regard, it should also be pointed out that

the case law of the Markets Court relied on by the second defendant implies that the

Litigation Chamber cannot seize new charges, because this would constitute a

violation of the rights of defense of the defendants. In this regard, the Chamber

Litigation recalls that in this case, no new offense was found and that the

pronounced relates only to the alleged violations of the GDPR already contained in the report

of the Inspection Service (see above).

236.

It should be noted that, in the contracts concluded between the two parties, the second

defendant was itself qualified by the latter as controller for the

so-called “second line” control and could therefore be presumed to act as such within the meaning of

Article 5.2 of the GDPR. Moreover, it appears from the documents in the file that the second defendant

did not contest its status as controller at the start of the procedure.88

237. Furthermore, the second defendant was given ample opportunity to defend itself - both in writing

only orally - during the proceedings before the DPA concerning the alleged infringements. The

second defendant also made use of this possibility, both during contacts with the

Inspection Service only by presenting its response dated 2 April 2021 and when

the hearing.

238. Contrary to what the second defendant asserts in its reaction to the application form

sanction, it was indeed aware of the fact that the responsibility for the processing in the

context of the disputed processing was the subject of debate during the proceedings before the Chamber

Litigation. In its response, the first defendant disputed the analysis according to which the

second defendant had to be qualified as a subcontractor. This point has also been widely

discussed during the hearing before the Litigation Chamber, where the second defendant declared

be of the opinion that the two analyzes - both that included in the contracts and the qualification by the

88 In this respect, it is possible to refer, inter alia, to the letter dated 30 September 2020 with the responses to

questions from the Inspection Service which the second defendant addressed to the aforementioned service.

Inspection service - were defensible, depending on the level of detail with which the purpose of the

treatment is determined.89

239. With regard to the second argument of the second defendant concerning the form of

sanction, the Litigation Chamber recalls that neither the GDPR nor the LCA contain a

additional obligation to grant the parties the possibility of presenting means of defense

concerning (the amount of) the envisaged sanction(s). However, the Litigation Chamber

has provided for this possibility on its own initiative in order to ensure maximum protection of

rights of defence, in accordance with the case law of the Court of Appeal of Brussels, Section

Court of Markets, in the matter. However, the Litigation Chamber is not bound, either by virtue of

of the GDPR or the LCA, nor under the aforementioned case law of the Court of Markets, of

submit the reasons for this decision to the defendants before taking the

decision in question.

240. With regard to the argument of the second defendant relating to the disproportionate nature

of the administrative fine, the Litigation Chamber recalls that under Article 83.4 of the

GDPR, infringements of articles 35.1 and 35.7 of the GDPR are subject to administrative fines

up to EUR 10,000,000 or 2% of total annual turnover for the financial year

previous. In accordance with Article 83.5 of the GDPR, infringements of Articles 5.1, 6.1 and 9.2 of the

GDPR are subject to administrative fines of up to EUR 20,000,000 or 4%

of the total annual turnover of the previous financial year.

241. The Litigation Chamber considers that it can base itself on the annual turnover of

the 2020 financial year of the second defendant to set the amount of the administrative fine.

242. On the basis of the conclusions submitted as well as the annual accounts filed with the

National Bank of Belgium (BNB), the Litigation Chamber finds that the turnover

for the 2020 financial year amounts to EUR 15,195,338.

242. The Litigation Chamber decides to maintain the administrative fine of 20,000 euros provided

in the penalty form. It emphasizes that the aforementioned fine is significantly lower than the

maximum amounts of 10,000,000 and 20,000,000 euros provided for in Articles 83.4 and 83.5 of the

GDPR. In addition, the fine is only 0.10% of the annual turnover of the first

defendant, which is significantly lower than the maximum percentages mentioned above

2 and 4% provided for in Articles 83.4 and 83.5 of the GDPR, which moreover only have the force of law for

fines exceeding the aforementioned maximum amounts.

89 See minutes of the hearing dated September 8, 2021.

243.

With regard to the second defendant's argument that only a small part of its

turnover would relate to the litigious processing activity and that the other activities did not

not been the subject of an investigation by the Inspection Service, the Litigation Chamber recalls that

Article 83 of the GDPR does not mention such a circumstance as a criterion to be taken into account

when imposing administrative fines by the supervisory authority.

244. The Litigation Chamber also emphasizes that the other criteria set out in Article 83.2 of the

GDPR are not likely in this case to lead to administrative fines other than that

that the Litigation Chamber has set in the context of this decision.

245. For breaches of Articles 5.2, 24 and 35.1 of the GDPR, the Litigation Chamber decides, in

pursuant to Article 100, §1, 5° of the LCA, to send a call to order to the first defendant.

IV. Publication of the decision

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

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

data in accordance with

article 95, §1, 8° of

the ACL, mentioning

the data

identification of the first and second defendants, due to the specificity of

this Decision - which leads to the fact that even in the event of omission of the data

identification, re-identification is inevitable - as well as the general interest of this decision.

Decision on the merits 48/2022 - 74/74

FOR THESE REASONS,

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

-

pursuant to Article 58.2 of the GDPR and Article 100, § 1, 13° of the ACL, to impose a

administrative fine of EUR 200,000 to the first defendant for violation of the

articles 5.1 c), 6.1 e), 9.2 g), 12 combined with art. 13.1 c), 13.2 e), 35.1, 35.3 and 35.7 b) of the

GDPR;

-

pursuant to Article 58.2 of the GDPR and Article 100, § 1, 13° of the LCA, to impose a

administrative fine of 20,000 euros to the second defendant for violation of the

Articles 5.1 c), 6.1 e), 9.2 g), 35.1 and 35.3 of the GDPR; and

-

pursuant to Article 58.2 b) of the GDPR and Article 100, § 1, 5° of the LCA, to send a

call to order to the first defendant for violation of articles 5.2, 24 and 35.1 of the

GDPR (due to the late finalization of the DPIA).

In accordance with Article 108, § 1 of the LCA, this decision may be appealed in

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

the Data Protection Authority as defendant.

(se). Hielke Hijmans

President of the Litigation Chamber