

Litigation Chamber

Decision on the merits 47/2022 of 4 April 2022

File number: DOS-2020-04002

Subject: Use of thermal cameras at Brussels South Charleroi Airport in

the framework of the fight against COVID-19

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

Chairman, and Messrs. Jelle Stassijns and Romain Robert;

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

of natural persons with regard to the processing of personal data and to the free movement

of this data, and repealing Directive 95/46/EC (General Data Protection Regulation),

hereinafter “GDPR”;

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

Having regard to the Law of 30 July 2018 relating to the protection of natural persons with regard to the processing of

personal data;

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: BSCA SA, whose registered office is located at 8 rue des Frères Wright, 6041 Charleroi, registered

.

.

under company number 0444.556.344, represented by Me Frédéric Deschamps

.

.□

and Me Nathan Vanhelleputt, hereinafter: "the defendant".□

Decision on the merits 47/2022 - 2/73□

I. Facts and procedure□

1. On August 28, 2020, the Inspection Service decided to take action on its own initiative in accordance with□

Article 63, 6° of the law of December 3, 2017 creating the Data Protection Authority.□

2. This decision follows serious indications of the use, by the public limited company Brussels South□

Charleroi Airport (hereinafter "BSCA S.A."), thermal imaging cameras to combat the□

spread of COVID-19. The decision was justified on the basis of the following elements in particular:□

- Articles and publications in various Belgian newspapers and media sites referring to□

thermal cameras used by BSCA S.A.;□

- Frequently asked questions (FAQs) published on the website of the Data Protection Authority□

data (hereinafter "APD") concerning the control of body temperature within the framework of the□

fight against COVID-19;□

- The press release published by the APD on its website¹ dated 17 June 2020 concerning□

contacting Brussels Airport regarding the temperature control carried out by this□

last ;□

- The possible processing of data concerning health which, according to the terms of the GDPR, "deserves□

higher protection"²;□

- The possible large-scale processing carried out;□

- The importance given by the DPA to processing operations concerning "the use of photos and cameras□

and "sensitive data"³ in accordance with its 2020-2025 strategic plan.□

3. On March 18, 2021, the investigation by the Inspection Service is closed, and its report is sent by□

the Inspector General to the President of the Litigation Chamber (art. 91, § 2 of the LCA).□

4. The report includes findings and retains the following offences:□

Finding 1: Violation of the principle of lawfulness of processing and necessity of the measure under□

of articles 5.1.a, 5.1.c., 6 and 9 of the GDPR

Finding 2: Violation of the principle of limitation of the purpose of the data in accordance with

Article 5.1.b. GDPR

Finding 3

: Violation of the principle of transparency and

the obligation to inform

in accordance with articles 5.1.a., 12 and 13 of the GDPR:

1 Available here: <https://www.autoriteprotectiondonnees.be/citoyen/controles-de-temperature-lapd-prend-contact-avec-brussels-airport>

2 GDPR, Recital 53.

3 Data Protection Authority, “Strategic Plan 2020-2025”, p.23.

Decision on the merits 47/2022 - 3/73

Finding 4: Violation of the obligation to carry out an impact study relating to the protection of

data before processing (violation of Article 35.1.):

Finding 5: Violation of the principle of confidentiality and the obligation to put in place

technical and organizational measures to secure the data (article 5.1.f and 32 of the

GDPR)

Finding 6: Violation of the principle of data protection by design and by default

(Article 25 of the GDPR):

Finding 7: Violation of the obligation to maintain a complete record of processing activities

Finding 8: Violation of the obligation to guarantee the independence of the Data Protection Officer

data in accordance with article 38.3. GDPR

5. On May 5, 2021, the Litigation Division decides, pursuant to Article 95, § 1, 1° and Article 98 to

the ACL, that the case can be dealt with on the merits. The defendant is informed of this by sending

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

They are also informed, under article 99 of the LCA, of the deadlines for submitting their

conclusions.□

6. The deadline for receipt of the defendant's submissions in response was set for June 16□

2021.□

7. On May 20, 2021, the defendant requested a copy of the file (art. 95, §2, 3° LCA), which was□

transmitted on May 31, 2021.□

8. The Defendant agrees to receive all communications relating to the matter via□

electronically and manifests its intention to make use of the possibility of being heard, in accordance□

in Article 98 of the LCA. It also requests an extension of the deadline for conclusions to September 1□

2021.□

9. By letter sent on May 31, 2021, the Litigation Chamber accepts an extension of the deadline for submissions□

to July 9, 2021. By email dated June 1, 2021, the defendant again requests an extension of the deadline□

of conclusions on 1 September.□

10. By email from the registry of the Litigation Chamber of June 4, 2021, the concluding party is invited to conclude□

for July 23, 2021.□

11. On July 23, 2021, the Litigation Chamber received the defendant's submissions in response.□

12. On September 6, 2021, the parties are informed that the hearing will take place on October 6, 2021.□

13. On October 1, 2021, the Litigation Chamber sends the defendant a list of□

questions in preparation for the hearing.□

Decision on the merits 47/2022 - 4/73□

14. At the request of the defendant, the hearing is postponed to October 22, 2021.□

15. On October 18, 2021, the defendant sends its answers to the questions of the Chamber□

contentious.□

16. On October 22, 2021, the parties are heard by the Litigation Chamber. Beyond the Elements□

already set out in its pleadings, the defendant puts forward additional elements,□

in particular on transparency and the Privacy Policy.□

17. On November 18, 2021, the minutes of the hearing are submitted to the parties.□

18. On November 25, 2021, the Litigation Chamber receives the defendant's remarks relating to
in the minutes.

19. On February 15, 2022, the Litigation Division informed the defendant of its intention to
impose an administrative fine and the amount thereof.

20. On March 9, 2022, the Litigation Chamber received the defendant's reaction concerning
the intention to impose an administrative fine and the amount thereof. These arguments are
summarized under point "III. Penalty".

II. Motivation

II.1. Preliminary considerations

21. The Litigation Chamber first emphasizes that this decision concerns the processing of
personal data in the context of the COVID-19 pandemic.

22. In the context of this health crisis, unprecedented measures involving the treatment of
(particular categories of) personal data have been and are being taken.

23. Given this crisis situation, the Litigation Chamber understands the urgency with which
some of these measures had to be taken by the competent authorities and bodies and had to be
implemented by the data controllers concerned. She also heard the
difficulties inherent in this situation. However, it should be emphasized that this does not detract from the fact
GDPR and other personal data protection legislation,
which constitute essential protection for the rights and freedoms of data subjects,
remain applicable. Crisis situations do not justify derogating from the requirements of the GDPR. At
On the contrary, in such circumstances, where individual freedoms are often threatened, it is
should comply with the legal framework which precisely makes it possible to avoid abuses and infringements of
fundamental rights.

Decision on the merits 47/2022 - 5/73

24. The monitoring role of ODA concerning technological, commercial or other developments⁴, as well as
that the prior opinions given by the knowledge center are without prejudice to the obligation

for data controllers to comply with the legislation in force and, if applicable, of a

sanction by the Litigation Chamber when this is not the case.

II.2. Preliminary questions regarding the quality of administrative authority of the Litigation Chamber of the Data Protection Authority

25. In these conclusions, the respondent raises three preliminary questions which will be addressed before questions on the merits.

II.2.1.

Lack of reasoning for the decision activating the processing of the case on the merits

26. The defendant indicates in its submissions that “the decision to deal with the case on the merits is not legally justified within the meaning of the law of July 29, 1991 relating to the formal motivation of acts administrative and case law of the Court of Appeal of Brussels, section Court of Markets”.

27. The case law of the Markets Court to which reference is made requires the

Litigation Chamber that “the motivation as it appears in the act sets out the considerations

legal and factual basis on which the decision is based and this rationale must be

enough to make the decision. This obligation to state reasons exists both from a formal point of view

than material. The Markets Court adds that “it is enough that the reasons are clearly, if necessary

concisely set out in the decision itself. »⁵

28. The Litigation Chamber finds that these conditions are met in the present case. Indeed, the

decision to deal with the case on the merits was communicated to the defendant by letter dated May 5

2021. The letter expressly indicates that the decision to deal on the merits follows the

findings made by the investigation report of the Inspection Service. The letter takes up the eight

findings of possible breaches of the GDPR noted by the Inspection Service and indicates that

these are subject to substantive review. The investigation report is also annexed to the

mail. In addition, the letter of May 5, 2020 indicates that the decision to deal with the case on the merits

is taken on the basis of articles 95, §1, 1° and 98 of the LCA.

II.2.2. The lack of independence and impartiality of the Data Protection Authority

29. The defendant maintains in its submissions that the Data Protection Authority in its

together fails in its duties of impartiality and independence. The defendant bases this

4 Article 10 of the LCA.

5 Brussels, (sect. Cour des Marchés), (19th chamber A), 21 January 2021, point 7.3, available at

<https://www.autoriteprotectiondonnees.be/publications/arret-du-27-janvier-2021-de-la-cour-des-marches-ar-1333.pdf>.

Decision on the merits 47/2022 - 6/73

argument on various press articles, relating conflicts within the Protection Authority

data as well as the opening of an infringement procedure by the European Commission.

30. The Litigation Chamber first notes that the Respondent invokes impartiality and

lack of independence of the Data Protection Authority in a very general way, without

refer to specific facts, a specific body or member of the Authority, and without linking its considerations

to any decision or administrative act taken by the Data Protection Authority in the

this file.

31. However, the defendant does not indicate at any time in what way the independence or the impartiality of

the Litigation Chamber could be called into question.

II.2.3. Misappropriation of power

Criticism of the content of the standard in the inspection report, the finding drawn therefrom and the

resulting misuse of power

32. The defendant contests in its conclusions that the Inspection Service can question

the form or substance of a legal norm enforceable in cases other than those provided for in Article 6

of the law of December 3, 2017. It formulates this criticism as follows:

“Therefore, by openly criticizing and questioning the legality of the Ministerial Order and

of the Protocol to draw therefrom the finding of a violation on the part of the conclusive, the service

of inspection calls into question the substance of the legal basis on which the conclusive relied for

process personal data. In fact, the inspection service

therefore calls into question the content of a standard enacted by the executive power in times of crisis

sanitary. »6

33. As part of its tasks set out in Article 4 of the LCA, the Data Protection Authority is

“responsible for monitoring compliance with the fundamental principles of data protection at

personal character”. One of the fundamental principles of the right to data protection

personal data is the principle of lawfulness, established in articles 5.1.a and 6 of the GDPR. This principle conditions

any processing of personal data to the existence of a basis of lawfulness, of which the

data controller must be able to demonstrate the existence under the principle of liability

listed in Article 24 of the GDPR.

34. In the present case, during the investigation by the Inspection Service and in its conclusions, the party

Defendant invoked Article 6.1.c) as a basis of lawfulness, which article is worded as follows:

“processing is necessary for compliance with a legal obligation to which the data controller

treatment is submitted”

6 Conclusions of the defendant, § 23.

Decision on the merits 47/2022 - 7/73

35. The Litigation Division recalls in this regard that, while the Inspection Service is the main body

of investigation of the APD7, and that only the Litigation Chamber has the competence to take

a decision based on the findings of the Inspection Service. There can therefore be no question of

misuse of power on the part of the Inspection Service, which has no decision-making power

at the bottom of the file.

36. In addition, compliance with the principle of lawfulness consists in examining whether the legal obligation claimed by the

data controller exists and if the processing is necessary to comply with this obligation

legal. It is therefore not a question, as the defendant maintains, of calling into question the Decree

ministerial and the Protocol8, but to check that the processing implemented by the person in charge

of processing are lawful and fall within the legal framework laid down by these legal instruments. If in

As part of its examination, the Litigation Chamber considers that the standard which would allegedly base

processing does not comply with the requirements of the GDPR, it may conclude that the processing is

illicit.□

37. This approach is also followed in the investigation report produced by the Inspection Service□

which indicates in particular that “during an examination aimed at knowing whether the processing is lawful, it is□
necessary to assess whether:□

-□

There is a reason of public interest in the field of public health in accordance with Article□

9.2.i. GDPR;□

-□

There is a legal provision that can be validly invoked by the person responsible for the□

processing in accordance with Articles 6.1.c., 6.3. and 9.2.i. GDPR;□

-□

The processing operations concerned are necessary for:□

- Comply with the legal obligation invoked in accordance with article 6.1.c. and ;□
- Reasons of public interest in the field of public health in accordance with Article□

9.2.i. GDPR." 9□

38. This wording makes it clear that it is indeed the processing whose lawfulness will be□

examined and not the validity of the standards themselves. This is confirmed by the wording of□

findings of the Inspection Service in its investigation. Indeed, the Inspection Service finds□

that the defendant processes personal data without an adequate legal framework in□

violation of Articles 6.1, 6.3 and 9.2.i of the GDPR, which clearly demonstrates that it is the processing that is□
considered contentious.□

7 Article 28 of the law of 3 December 2017 establishing the Data Protection Authority.□

8 FPS Mobility and Transport of Belgium, “Commercial Passenger Aviation” Protocol (see point 62 et seq.).□

9 Investigation report, p 25.□

Decision on the merits 47/2022 - 8/73□

39. On the basis of these considerations, the defendant's argument based on a possible misappropriation of□

power must be discarded.□

The fact that any financial fine would constitute a misuse of power□

40. Based on the case law of the Court of Markets, the defendant indicates that "since the□

conclusive has never received a compliance injunction or any other sanction and that the□

processing concerned by this procedure has ended since October 15, 2020 for the controls□

arrivals and March 21, 2021 for departure controls, it should be considered that any□

financial penalty would constitute, on the part of the Litigation Chamber, a misappropriation of□

power within the meaning of the case law of the Court of Appeal of Brussels, Market Court section".□

41. The Data Protection Authority has, like all supervisory authorities, the power to impose□

administrative fines to ensure the effective application of the GDPR, under the text-□

even GDPR. As can be seen from recital 148, an administrative fine can be□

imposed in addition to or instead of the appropriate measures that are imposed10. Bedroom□

Contentieux acts in this case pursuant to Article 58.2.i) of the GDPR. The possibility of imposing□

an administrative fine is therefore in no way subordinated to an injunction□

prior compliance. This would call into question the effectiveness of the application of the GDPR if the□

data controllers could take refuge behind the absence of prior formal notice□

to escape a fine. To this end, the GDPR and the LCA provide for several measures□

corrections, including the orders cited in Article 100, § 1, 8° and 9° of the LCA. It is for the authority to□

control to choose the appropriate measure to guarantee an effective application of the GDPR, in□

exercising its discretionary power in this respect11, framed in particular by the procedural guarantees□

and that fines must be "effective, proportionate and dissuasive".12□

10 Recital 148 provides the following: "In order to strengthen the application of the rules of this Regulation, sanctions including□

administrative fines should be imposed for any violation of this Regulation, in addition to or instead of the□

appropriate measures imposed by the supervisory authority under this Regulation. In the event of a minor violation or if the fine□

liable to be imposed constitutes a disproportionate burden for a natural person, a warning may be issued□

rather than a fine. However, due consideration should be given to the nature, gravity and duration of the breach, the character□

intent of the breach and the measures taken to mitigate the damage suffered, the degree of responsibility or any breach
relevant previously committed, the manner in which the supervisory authority became aware of the breach, compliance with
measures ordered against the controller or processor, the application of a code of conduct, and any
other aggravating or mitigating circumstance. The application of sanctions, including administrative fines, should be subject to
appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to
effective judicial protection and due process. See also European Protection Board guidelines
data on the application of administrative fines of October 3, 2017, WP 253, which confirms that the authorities can
choose to combine several measures, including an administrative fine.

11 Court of Markets, NDPK t. GBA, 7 July 2021. Available at: <https://www.autoriteprotectiondonnees.be/publications/arret-du-7-july-2021-de-la-cour-des-marches-ar-320-available-in-dutch.pdf>

12 Article 83.1 GDPR.

Decision on the merits 47/2022 - 9/73

II.3. As for the background

II.3.1 Identification of disputed processing and applicability of the GDPR

42. It appears from the documents in the file and from the investigation report of the inspection service that the file bears
on temperature checks carried out by the defendant at Brussels South airport

Charleroi in the context of the COVID-19 pandemic.

43. The system put in place consists of two distinct procedures: one at the level of departures, the other
at the arrivals level.

44. With regard to the level of departures, the defendant set up a control of the
temperature of all passengers and any accompanying persons on departure from the airport
of Brussels South Charleroi. Two thermal cameras are installed in the pre-check tent. A
first temperature is taken using these cameras. The device is monitored by X
and by the defendant's firefighters.

45. In the event of a temperature above 38°C, a second test is carried out on the person concerned by
staff monitoring screens using a digital forehead thermometer. If the temperature is

again above 38°C, the passenger is invited to go to the infirmary or a new outlet□

temperature will be taken using a digital thermometer under the arm. If on this third occasion□

the temperature again exceeds 38°C, the fire department is notified by radio or by 112. A□

firefighter intervenes to take the anamnesis of the person concerned. This consists of putting□

additional questions to the passenger to determine if they are suffering from other symptoms of□

type COVID 19. The exchange takes place orally without taking notes.□

46. If this leads to a suspicion of COVID and if the airline he is flying with prohibits□

boarding to passengers with a fever, the passenger will not be able to access the terminal.□

47. The system was put in place from June 15, 2020. It was operational during business hours□

airport opening hours (between 4:00 a.m. and 9:00 p.m.). Until November 6, X intervened in the□

process. From that date, the task was taken over by the firefighters-ambulance of the□

defendant. Controls ended on March 22, 2021. Between June 15, 2020 and October 31□

2020, approximately 457,000 departing passengers were screened.□

48. X also had to complete a document every day showing the number of passengers whose□

temperature was above 38°C, as well as the temperature of these same passengers. The document□

did not contain the surnames or first names of these people and it was destroyed every week.□

49. At the arrivals level, the system was operational from September 7, 2020 to October 15, 2020. It□

consisted of using 6 thermal cameras to monitor the temperature of passengers coming□

of a red zone. The device was under the supervision of X and the fire-paramedics. In case□

Decision on the merits 47/2022 - 10/73□

temperature above 38°C, the passenger received a document inviting him to pay attention to□

other potential symptoms of COVID and to contact a doctor if desired.□

50. According to the defendant, the system was only put in place when there was a return flight from a□

Red zone. The defendant indicates that it is unable to determine the number of people□

concerned returning from a red zone and having undergone a temperature check□

bodily.□

51. Thermal cameras are equipped with software that sends an alert when a temperature greater than or equal to 38°C is detected. An image of the passenger with his mask then appears in the computer's event center. At the request of the defendant, the cameras are configured for a pre-alert at 37.5°C and an alert at 38°C.

52. Camera software temporarily caches the last twenty alert images. These are deleted at the end of each day.

53. The Inspection Service notes that the thermal camera system as set up by BSCA S.A. must therefore be considered as an automated personal data process personnel falling within the material scope of the GDPR in accordance with Article 2.1. from GDPR, as it involves taking an image of passengers with a temperature above 38°C using thermal imaging cameras.

54. The Inspection Service also notes that the processing concerned in the context of this report involve health data within the meaning of Article 4.15. of the GDPR, since they reveal an aspect relating to the physical health of people, namely fever. The Inspection Service also believes that the oral history is likely to contain other information to medical character.

55. The defendant did not dispute these two findings made by the Service of Inspection. The Litigation Chamber specifies, however, that the disputed data processing is limited to images taken by thermal cameras. The subsequent stages of the process (taking temperature without image and the anamnesis), do not constitute data processing to personal character within the meaning of articles 2.1, 4.1 and 4.2 of the GDPR. Indeed, taking the temperature via manual thermometer does not constitute a processing of personal data within the meaning of article 4.2 of the GDPR, since it was not, to the knowledge of the Litigation Chamber, the subject of any operation mentioned in this article¹³.

¹³ The recording and/or communication of information resulting from manual temperature taking and anamnesis to any recipient (such as an airline) would however constitute such processing.

II.3.2 Identification of the data controller

56. The Inspection Department finds that BSCA S.A. must be considered to be responsible for the processing for the processing examined in the context of this file in accordance with Article 4.7. of the GDPR. To reach this conclusion, the Inspection Service relies on the fact that the defendant recognizes this quality itself and that it concluded a contract both with X and with I-CARE SPRL for the supply of thermal cameras.

57. This finding has not been contested by the defendant. The Litigation Chamber follows moreover the Inspection Service in this regard.

II.3.3 Finding 1: Violation of the principle of lawfulness of processing and necessity of the measure under Articles 5.1.a, 5.1.c., 6 and 9 of the GDPR

Findings of the Inspection Service

58. It appears from the investigation report that the defendant claims Articles 6.1.c) and 9.2.i) of the GDPR as bases for the lawfulness of the processing. These two articles are reproduced below:

“Clause 6

Lawfulness of processing

1. Processing is only lawful if and insofar as at least one of the following conditions is

filled:

[...]

c) processing is necessary for compliance with a legal obligation to which the data controller treatment is submitted; »

“Clause 9

Processing of special categories of personal data

1. The processing of personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as that the processing of genetic data, biometric data for the purpose of identifying a

natural person in a unique way, data concerning health or data

concerning a natural person's sex life or sexual orientation is prohibited.

2. Paragraph 1 does not apply if one of the following conditions is fulfilled:

Decision on the merits 47/2022 - 12/73

[...]

i) the processing is necessary for reasons of public interest in the field of health

public, such as protection against serious cross-border threats to the

health, or for the purpose of ensuring high standards of quality and safety of health care

and medicinal products or medical devices, on the basis of Union law or the law of

the Member State which provides appropriate and specific measures for the safeguarding of

rights and freedoms of the data subject, in particular professional secrecy”.

59. Regarding the legal obligation of Article 6.1.c, the investigation report indicates that the respondent

is based on Article 4 of the Ministerial Order on emergency measures to limit the

spread of the COVID-19 coronavirus of June 30, 2020. This ministerial decree followed

several similar ministerial orders and was subsequently replaced by a succession of other

ministerial orders. The most recent at the time of writing the investigation report is the decree

of 28 October 2020. It was only during the investigation by the Inspection Service that the

reference to these legal bases was put forward by the complainant.

60. Article 4 of the ministerial decree of June 20 was worded as follows:

“Without prejudice to Article 5, companies and associations offering goods or services to

consumers and, from 1 September 2020, the organizers of trade fairs, in

including lounges, operate in accordance with protocol or minimum rules

which have been communicated on the website of the competent public service. [...]”.

61. This article was repealed by a ministerial decree of October 18, 2020, article 5 of which reproduced article

4 of the ministerial decree of June 30, 2021. This decree was then replaced by a ministerial decree of

October 28, 2020, Article 5 of which reads as follows:

“Without prejudice to Article 8, companies and associations offering goods or services to

consumers operate in accordance with the protocol or minimum rules that

have been communicated on the website of the competent public service. ”.

62. These ministerial orders successively provide that companies and associations offering

goods or services to consumers, operate in accordance with the protocol

or the minimum rules that have been communicated on the website of the competent public service. the

Protocol applicable to the defendant is a protocol entitled “Commercial Aviation

passengers” which emanates from the FPS Mobility and Transport of Belgium (hereinafter: the Protocol).

14 Ministerial decree of June 30, 2020 on emergency measures to limit the spread of the COVID-19 coronavirus.

15 Ministerial Order of October 28, 2020 on emergency measures to limit the spread of the COVID-19 coronavirus.

63. The Protocol contains on page 5 specific sanitary measures applicable to airports and

in particular, the following measure:

Decision on the merits 47/2022 - 13/73

64. The Inspection Service also notes that the Protocol contains the following provision:

65. The paragraph regarding passenger temperature checks copied above can be found

under Chapter 2 of the Protocol.

66. The Inspection Service noted that on 12 October 2020, the Protocol was published on the

FPS Mobility and Transport website.

67. It emerges from the investigation report that with regard to the grounds of public interest in the field of health

public in accordance with Article 9.2.i. of the GDPR, the defendant specifies that this concerns in particular

“the protection against serious cross-border threats to health, in this case the epidemic

of COVID-19”. In this regard, it indicates that recital 46 of the GDPR explicitly mentions the

fight against epidemics.

68. In addition, the defendant indicated (exhibit 7) that this processing falls within the legislative framework put in place

place, namely the Ministerial Order of 30 June 2020 and the Protocol.

69. Based on Articles 5.1.a, 6.1, 6.3 and 9.2.i) of the GDPR, the Inspection Service considers that in order to

to ensure the lawfulness of the processing, it is necessary to assess the elements below.□

Decision on the merits 47/2022 - 14/73□

70. Firstly, the Inspection Service considers that the fight against the spread of COVID-19 must□

be considered a public interest in the field of public health in accordance with□

Article 9.2.i of the GDPR.□

71. Secondly, the Inspection Service considers that the data is processed without a framework□

legal, in violation of articles 6.1.c, 6.3 and 9.2.i) of the GDPR and that it is therefore□

illicit. To reach this conclusion, the Inspection Service relies on the following elements:□

- The purpose of the norm invoked has not been determined by law and the Protocol defines by□

elsewhere a purpose different from that of the ministerial decree;□

- The basic methods of measuring body temperature have not been defined by the□

law ;□

- The predictability of the Protocol is problematic given the lack of publication;□

- The standards invoked are not a law in the proper sense;□

- The standards invoked do not provide any supervision of the processing by guarantees.□

72. Thirdly, the Inspection Service considers that the medical necessity of the checks□

passenger body temperature is disputed.□

Position of the defendant□

73. In its submissions, the defendant recalls the legal framework for data processing which is□

made up of successive ministerial decrees, as well as the Protocol, the latter being binding on the□

defendant.□

74. The defendant also considers that the existence of a public interest in the field of health□

public on the basis of Article 9.2.i is well proven in this case.□

75. It also considers that there is a legal provision which can be validly invoked by the□

controller in accordance with Articles 6.1.c, 6.3 and 9.2.i) of the GDPR.□

76. It relies on the following four elements to support this:□

- First of all, as already explained above (point 32 et seq.), the defendant considers that it

it is not for the Inspection Service to comment on the validity of a legal standard or

enforceable. It is solely up to him to verify that a legal obligation exists, making the

valid processing according to article 5.1.c (sic) of the GDPR.

- Then, she indicates that the temperature checks were imposed on her by the Protocol, itself

even made compulsory by Ministerial Orders. The defendant expresses for the

first time that these ministerial decrees are based on article 4 of the law of December 31

Decision on the merits 47/2022 - 15/73

1963¹⁶ (hereinafter, law relating to civil protection) and the law of 15 May 2007¹⁷ (hereinafter, law relating to

civil security). The defendant indicates that these laws have been validated by the Council of State

as a legal basis for ministerial decrees. The defendant also indicates, for the

first time in its conclusions, relying on the decree of 23 June 1994¹⁸ (hereinafter, the decree

Walloon). She adds that the ministerial decrees were validated by the Council of State in a judgment

of October 30, 2020¹⁹. The defendant states that it participated in the workshops for the development of the

Protocol, with the FPS Mobility, the airports and the main Belgian airlines.

- With regard to the purpose, the basic modalities and the delay of the publication, the

defendant considers that it cannot be held responsible for compliance with these obligations

(which are not required by Article 9.2.i) of the GDPR) and that these do not affect its

obligation to implement the measures laid down in the Protocol.

- As for the requirement of necessity of the processing, the defendant considers, like the Service

of Inspection that it is not up to the DPA to decide on the medical necessity of the

thermal cameras to fight COVID-19. The defendant also wonders

on the possibility of carrying out such an analysis a posteriori, recalling the uncertainty that prevailed at

the time. She adds that no other pragmatic solution existed at the time for him

allow him to comply with the prescriptions of the Protocol imposed on him. She indicates

also that it was not carrying out COVID tests as such, but rather

temperature controls. According to her, the term “positive/negative test” has no reason to exist.□

She adds that no less than 65 other European airports have implemented such systems.□

and that these have, moreover, been interrupted at her home for months (see paragraphs 47 and 49). She□

adds that it does not derive any interest from the processing of its data and that the risk that these□

present is otherwise very limited. She concludes that the treatment was at the time□

necessary and proportional to the purposes of such processing.□

77. During the hearing, the defendant clarified in particular that the cessation of the temperature measurement was□

decided due to greater use of PCR tests, the establishment of quarantines as well□

only for financial considerations.□

78. The defendant specifies that with regard to departures, only three people have, following the□

temperature taking process, were asked not to enter the terminal. If these people□

16 Law of 31 December 1963 on civil protection.□

17 Law of 15 May 2007 on civil security.□

18 Decree of 23 June 1994 relating to the creation and operation of airports and aerodromes within the Walloon Region□

19 Decision of the Council of State of October 30, 2020, 248.818, available at [http://www.raadvstconsetat.](http://www.raadvstconsetat.be/arr.php?nr=248818)□

[be/arr.php?nr=248818.](http://www.raadvstconsetat.be/arr.php?nr=248818)□

20 Comments on the minutes of the hearing of October 22, 2021, p. 1.□

Decision on the merits 47/2022 - 16/73□

had nevertheless wished to do so, their identity would have been communicated to the company□

Aerial. The final decision whether or not to allow boarding would have belonged to the captain□

board, under international law.□

79. Then concerning the legal basis and the Protocol, the respondent argued during the hearing□

that it was subject to a legal obligation on the basis of the Protocol, although it considers that this□

Protocol suffers from drafting blunders which could give rise to interpretations□

different. The defendant adds that it was not, moreover, involved in the drafting of the□

Protocol and moreover believes that a law would have been more appropriate²¹. She adds that the lines□

EASA guidelines are also not always the clearest.²² She adds that she has

requested intervention from the public authorities as to the lawfulness of the processing following the launch of investigation by the Inspection Service.

Examination by the Litigation Chamber

80. The Litigation Chamber emphasizes that the processing of personal data is only lawful only if it is carried out on a legal basis provided for in Article 6.1 of the GDPR.

81. Since it has been found in this case (see above) that the screening system has also involved the processing of special categories of personal data (more specifically data concerning the health of the persons concerned within the meaning of article 4.15 of the GDPR), data controllers must also demonstrate that one of the grounds for exception the principle of the prohibition of processing for this type of personal data, set out in GDPR Article 9.2 applies. As the Litigation Chamber has already estimated²³,

processing of special categories of personal data within the meaning of Article 9 of the GDPR must indeed be based on Article 9.2 of the GDPR, read in conjunction with Article 6.1 of the GDPR. This has been established by the European Commission and the EDPB²⁴ and is also confirmed by the recital 51 of the GDPR, which provides the following regarding the processing of special categories of personal data: "In addition to the specific requirements applicable to this processing, the

²¹ Comments on the minutes of the hearing of October 22, 2021, p. 2.

²² See also the response to the Inspection Service of 24 November 2020.

²³ Cf. substantive decision 76/2021, point 33, available at: <https://www.autoriteprotectiondonnees.be/publications/decision-as-to-fund-n-76-2021.pdf>.

²⁴ On this subject, see GEORGIEVA, L. and KUNER, C., "Article 9. Processing of special categories of personal data" in KUNE L.A. en DOCKSEY, C., The EU General Data Protection Regulation (GDPR). A commentary, Oxford University Press, Oxford, p. 100. 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'.²⁴

Decision on the merits 47/2022 - 17/73²⁵

general principles and the other rules of this Regulation should apply, in particular in
with regard to the conditions of lawfulness of the processing".²⁵

Regarding the application of Articles 6.1.c) and 9.2.i) of the GDPR to the present case²⁶

82. In the present case, during the exchanges with the DPA, the controller claims to rely
on Article 6.1.c) of the GDPR and Article 9.2.i).²⁷

83. The Litigation Chamber emphasizes that in order to be able to validly invoke the basis of lawfulness of
Article 6.1.c) and the exception provided for in Article 9.2.i) of the GDPR, the controller must
demonstrate :²⁸

(i)²⁹

that there is an important reason of public interest in the field of public health (article 9.2.i)
;

(ii)³⁰

that there is a legal provision that can be validly invoked by the person responsible
processing in accordance with Articles 6.1.c, 6.3 and 9.2.i) of the GDPR.³¹

(iii)³²

That the processing operations concerned are necessary to³³

o Comply with the legal obligation invoked in accordance with Article 6.1.c and³⁴

o Reasons of public interest in the field of public health in accordance with
Article 9.2.i).³⁵

84. With regard to the first constituent element of Article 9.2.i) of the GDPR, namely the existence of a
"important public interest in the field of public health", the Inspection Service does not³⁶
does not question in his investigation report the presence of such an interest in this case. Bedroom³⁷
Litigation observes in this respect that it is indeed a question of a "significant public interest in the³⁸

field of public health" within the meaning of Article 9.2.i) of the GDPR. The Litigation Chamber considers
indeed that there can be no doubt that the fight against the Covid-19 pandemic
should be considered as such. As also invoked by the defendant, this is explicitly
formulated in recital 46 of the GDPR, which mentions "[monitoring] epidemics and their spread"
as an "important cause of public interest".

85. The second constituent element concerns the existence of a legal provision on which the
processing in accordance with Articles 6.1.C and 9.2.i) of the GDPR.

86. 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 compliance with a legal obligation²⁶ and/or to
the performance of a task in the public interest or in the exercise of official authority

²⁵ Highlighting is by the Litigation Chamber.

²⁶ Article 6.1.c) of the GDPR.

Decision on the merits 47/2022 - 18/73

vested in the controller²⁷ must be governed by clear and precise regulations whose
the application must be foreseeable for the persons concerned.

87. Article 6.3 of the GDPR provides more precisely the following in this regard: "The basis for the processing
referred to in points (c) and (e) of paragraph 1 is defined by: (a) Union law; or (b) the law of the Member State
to which the controller is subject. The purposes of the processing are defined in this
legal basis or, with regard to the processing referred to in paragraph 1, point e), are necessary to
the performance of a task in the public interest or in the exercise of official authority
vested in the controller."

88. Recital 41 of the GDPR specifies in this respect: "Where this Regulation refers to a
legal basis or to a 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 order
constitution of the Member State concerned. However, this legal basis or measure
legislation 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 the European Union (hereinafter referred to as the "Court of Justice") and the European Court of Human Rights. »

89. As regards the legal basis invoked by the defendants, it must be noted that neither the decree relating to the creation and operation of airports and aerodromes, nor the ministerial decree or the law on civil security (see points 59 and s. and 76 and s. above) do not govern the disputed processing as such. This processing is provided for in the Commercial Aviation Protocol, adopted by the Federal Public Service Mobility and Transport (DG Air Transport), after negotiation with the sector concerned. This emerges from the wording of Article 1, 3° of the ministerial decree: "protocol": the document determined by the competent minister in consultation with the sector concerned (...). This also emerges from the documents in the file as well as from the email sent by the Minister's office competent to airport operators, airlines and regional authorities on 11 June 2020. The Litigation Chamber argues that in the context of Article 6.3 and considering 41 of the GDPR, cooperation and consultation with the sector are not in themselves a hindrance, provided that the obligation is imposed explicitly by a law in the broad sense. However, this was not the case in species (see below).

90. The Litigation Division refers more particularly in this respect to the Privacy International judgment of the Court of Justice of 6 October 2020, in which the Court states that the legislation in question must contain clear and precise rules "governing the scope and application of the measure in question and imposing minimum requirements, so that persons whose personal data personnel are concerned have sufficient safeguards to effectively protect these data against the risk of abuse." And the Court added: "This regulation must be legally binding in domestic law and, in particular, indicate in what circumstances and under Article 6.1.e) of the GDPR.

Decision on the merits 47/2022 - 19/73

under which conditions a measure providing for the processing of such data may be taken, thereby ensuring that the interference is limited to what is strictly necessary. (...) These considerations are valid

particular when the protection of this particular category of personal data is at stake.□

personal sensitive data".□

91. With regard to the aforementioned standards, the Respondent asserts in its submissions in response that□

by its judgment of October 30, 2020, the Belgian Council of State "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."□

however, to point out that the judgment in question does not concern the use of this legislation as□

legal basis for the processing of (special categories of) personal data and not□

does not constitute a verification of the aforementioned standards in the light of the GDPR. The judgment concerns□

the closure imposed on restaurants and drinking establishments in the context of Covid-19 and is no longer□

therefore not relevant to the present case. More importantly, the judgments of the Council of State bear□

on the legality of the measures imposed by ministerial order. However, it is clear that the decrees□

ministerial positions have a clear normative value on the Belgian right. This is not the case with the Protocol□

in question.□

92. This is confirmed by the Belgian Council of State in its opinion no. 69.253/AG of 23 April 2021, issued by□

the general meeting of the legislation section, which takes a position as follows:□

93. "Indeed, one of two things: either the protocols are not regulatory in nature, but in□

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

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

the initiation of public action in the event of non-compliance; either the protocols are actually□

of a regulatory nature and the measures they contain are indeed binding, but in□

In this case, these measures must be included in the decrees of the competent authority in the matter. »28□

94. This position of the Council of State follows the response of the minister's delegate, who asked about the□

legal quality of the protocol replied as follows:□

95. "De protocollen en gidsen vormen een indicatief beoordelingskader. From protocollen to gidsen□

kunnen enkel verordenende maatregelen, zoals bepaald in het MB, concretiseren, maar zijn zelf niet□

verordenend".29□

96. The Litigation Chamber further notes that the French Council of State stated the following with regard to the processing of special categories of personal data by means of cameras

28 This paragraph was repeated by the Council of State in Opinion 69.305 of May 6, 2021. Opinion No. 69.253/AG of April 23, 2021, an opinion issued by the Council of State on successive ministerial decrees (see point 62 et seq.). The opinion of the Legislation Section of the Council of State of April 23, 2021, on the request for an opinion on the draft law on the status of the French Republic of status not having been requested before, in view of the urgency. This is therefore the first opinion issued by the Council of State on the protocols provided for by this succession of ministerial decrees.

29 Legislation section of the Council of State, n° 69.253/AG of April 23, 2021, p. 42. Free translation: "Protocols and guides constitute an indicative assessment framework. Protocols and guides can only concretize regulatory measures, such as those stipulated in the AM [ministerial decree], but are not themselves regulatory".

Decision on the merits 47/2022 - 20/73

thermal without a valid legal basis: "it is not possible to estimate that the legal conditions of a processing of personal health data 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"³⁰.

97. During the hearing, the respondent also indicated that it considered that the legal basis was not the clearest and that a law would have been more judicious.

98. The Litigation Division therefore finds that the Protocol does not provide a valid legal basis for the processing within the meaning of Article 6.1 of the GDPR.

99. As a superabundant point, concerning the non-binding nature of the protocol invoked, the Chamber in litigation finds, on the basis of the documents, the following elements:

- The Protocol specifies that "EASA and ECDC do not recommend taking the temperature of passengers to allow them to travel with 'immunity passports'. The agency recalls that the relevance of this test is not supported by current scientific knowledge about the spread of SARS-CoV-2. Nevertheless, EASA and ECDC monitor scientific developments and will update their recommendations as appropriate if a suitable test becomes available.

Charleroi Airport (Brussels South Charleroi Airport), on request from airlines

airlines operating there, however, took the decision to implement the tests for taking
temperature of people entering the terminal. The airport guarantees that the method
chosen will not lead to delays or concentration of people at the entrance to its
infrastructure. »³²

- The airport took the initiative twice to interrupt treatment. This emerges from his
answer to the questions of January 6, 2021 where it indicates that the temperature measurement on arrivals has
was interrupted on October 15, 2020 at the initiative of the airport. With regard to arrivals, the
defendant indicated in its letter of October 18, 2021 that "The defendant interrupted
the temperature control system at the departures level from March 22, 2021 due to the
additional measures to combat the spread of the coronavirus put in place by the
different national governments. This was repeated during the hearing, since the defendant
y clearly states that when treatment is discontinued in March 2021, "the discontinuation is a
decision of BSCA"³³.

³⁰ French Council of State, order of 26 June 2020, n° 441065. Available at: [https://www.conseil-etat.fr/decisions-de-
justice/latest-decisions/council-of-state-june-26-2020-thermal-cameras-in-lisses](https://www.conseil-etat.fr/decisions-de-justice/latest-decisions/council-of-state-june-26-2020-thermal-cameras-in-lisses)

³¹ See paragraph 79 above.

³² It is the Litigation Chamber which underlines.

³³ Comments on the minutes of the hearing of October 22, 2021, p. 1.

Decision on the merits 47/2022 - 21/73

100. For the Litigation Chamber, these elements demonstrate, beyond the question of the existence of a
legal basis, the absence of a binding nature of the Protocol as regards specifically
temperature taking.

101. In addition, the Litigation Chamber considers that the Protocol does not meet the requirements imposed
by Article 6.3 of the GDPR and by European case law for the reasons listed below.

The purpose(s) of the disputed processing is (are) not mentioned in any way
sufficiently clear and consistent in the standards invoked

102. As mentioned above, under Article 6.3 of the GDPR, the basis for the processing referred to in paragraph 1, points c) and e) must be defined by Union law or by the law of the Member State to which the controller is subject. Recital 45 specifies that: "It should also belong to Union law or to the law of a Member State to determine the purpose of the processing. In addition, this law could specify the general conditions of this regulation governing the lawfulness of the processing of personal data, establish the specifications aimed at determine the data controller, the type of personal data subject of the processing, the persons concerned, the entities to which the personal data personal data can be communicated, the limitations of the purpose, the retention period and other measures to ensure lawful and fair processing. It should also belong to the Union law or the law of a Member State to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be an authority or another natural or legal person governed by public law (...)"³⁴.

103. The Litigation Division notes, however, that the standards invoked by the defendants do not clearly and unequivocally contain the precise purpose of the processing. They do not contain nor the basic processing methods as listed in paragraph previous.

104. With regard to the ministerial decree of June 5, 2020, the decree relating to the creation and operation of airports and aerodromes and the law relating to civil security, it is clear that none of these three standards do not mention the disputed processing. It is apparent from the wording of the decree ministerial that the purpose of the measures included therein is to "limit the spread of coronavirus COVID-19".

105. Even the Commercial Aviation Protocol – which does refer to the disputed processing – does not does not include a clear description of the purpose of the aforementioned processing. At most we can deduce of the title of the document that the purpose of the measures it contains is "the resumption of activities relating to commercial aviation for passengers".

34 Emphasis by the Litigation Chamber.□

Decision on the merits 47/2022 - 22/73□

The terms of the treatment have not been defined by the Protocol□

106. As indicated above, in accordance with Article 6.3 of the GDPR, read in conjunction with Article 22□

of the Constitution and with Articles 7 and 8 of the Charter of Fundamental Rights of the Union□

European Union, a legislative standard must define the essential characteristics of the processing of□

data, necessary for the performance of a task in the public interest or in the exercise of authority□

public authority vested in the controller. In the aforementioned provisions, it is emphasized□

In this regard, the processing in question must be framed by a sufficiently clear and□

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

107. However, the Commercial Aviation Protocol in no way sets out the essential elements of the□

disputed treatment. This leaves controllers a wide margin of appreciation as to□

how body temperature measurement should be performed. The Protocol leaves from□

airport managers the freedom to carry out this screening with or without processing□

personal data and even to define the other modalities, such as the number of□

temperature measurements, the technology used, the type and quantity of data processed and the duration□

retention of their data.□

The predictability (or unpredictability) of the Commercial Aviation Protocol□

108. European case law imposes the requirement of predictability of legislation. Standards□

invoked must also be sufficiently accessible for the persons concerned thanks to□

their publication, in particular also with regard to the nature and legal consequences for□

the person concerned.□

109. In this regard, it should be noted that the Protocol does not define the consequences for the□

data subject who refuses to submit to temperature screening. This element does not stand out□

as common EASA and ECDC operational guidelines. The purpose of the identification and□

the principle of control with image recording does not come out of the Protocol either. In□

Furthermore, the Protocol was not published on time and correctly. It was indeed published on the website

Internet of the Federal Public Service Mobility and Transport after its implementation.

110. The fact of not determining these modalities in the standard or the instrument invoked generates

significant derived risks for the rights and freedoms of data subjects (e.g.

confusion of purposes as well as an obstacle to the exercise of the rights of the persons concerned).

In accordance with the aforementioned case law of the Court of Justice (the Privacy International judgment), this does not

does not meet the requirement to provide by law (even in the broad sense) measures

Decision on the merits 47/2022 - 23/73

appropriate and specific for

safeguarding fundamental rights and

freedoms

fundamentals of the person concerned.

111. The Litigation Chamber takes note of the urgency with which the measures were taken in the

framework of the fight against the Covid-19 pandemic. She stresses, however, that this does not bear

prejudice to the fact that the requirements of the aforementioned provisions, which constitute

essential protection for the rights and freedoms under the law relating to the protection

personal data.

112. As data controllers, the Respondent is responsible, under the principle of

responsibility set out in Articles 5.2 and 24 of the GDPR ("accountability"), compliance with the principles of

protection of personal data (including the principle of lawfulness and necessity) and must

be able to demonstrate compliance with its legal obligations. The Litigation Chamber reminds

again that the defendant has recognized the lack of clarity of the Protocol³⁵.

113. The Litigation Chamber emphasizes that the defendant therefore had to ensure, from the start of the

disputed processing, to have a reason for lawfulness and a valid exception within the meaning respectively

of Articles 6.1 and 9.2 of the GDPR. The analysis of the documents in the file shows that this basis of legality

was not explained at the start of the treatment. This is also apparent from the absence

concrete reference to the legal basis in question in the privacy statement of the
defendant (see below).) It was only during the investigation by the Inspection Service that it was
mentioned for the first time, then integrated in an incomplete way in the policy of
confidentiality from December 2.

114.

It should also be emphasized that the legal norms invoked by those responsible for the
processing do not entail any obligation and do not create any legal framework for the performance
temperature control with recording of personal data.

115. The Litigation Chamber therefore concludes that the second constituent element is therefore not established.

116. With regard to the third constituent element, namely that the processing operations concerned must
be necessary to comply with the legal obligation invoked in accordance with Article 6.1.c and to
grounds of public interest in the field of public health in accordance with Article 9.2.i..

117. The Litigation Division considers above all that the reference to other similar processing in
65 other European airports is not relevant as proof of compliance with the requirement of
necessary in this case. In this respect, it is pointed out that the enumeration included in the
conclusions of the first defendant also implies that a (significant) number of airports (including
Belgian airports too) made no use of the temperature control system. The
Litigation Chamber further notes that the Protocol indicates that the processing was to be carried out

35 See paragraph 76 above.

Decision on the merits 47/2022 - 24/73

place in only two airports in Belgium (Charleroi airport and Zaventem airport) without
mention the other airports present on Belgian territory.

118. As regards compliance with the principle of necessity in the context of the processing at issue, the
Litigation Chamber emphasizes, like the defendant, that it cannot comment on
the medical necessity of this measure in the context of the fight against Covid-19 as such,
nor as to the scientific accuracy of the views and reports cited above. This analysis is not

however not necessary to be able to consider the necessity of the processing from a point of view

legal.

119. The Litigation Chamber notes, however, that the Commercial Aviation Protocol of the

Minister of Mobility – both in its version of June 11, 2020 and in that of July 31, 2020 –

mentions the following on page 5:

“Measuring the body temperature of passengers so that they can travel with a

“immunity passport” is not recommended by EASA and ECDC. EASA recalls that the

relevance of this measure is not supported by current scientific knowledge of the

SARS-CoV-2. (...)”³⁶

120. The Litigation Division therefore finds that the legal basis invoked by the defendant

itself mentions that the necessity of the processing concerned has not been established. She therefore concludes

that the necessity of the processing, as required by Articles 6.1 c), 6.3 and 9.2.i) of the GDPR is not

established.

121. Therefore, the Litigation Chamber holds in this case that the Commercial Aviation Protocol and

the other standards invoked by the defendant do not constitute a valid basis for treatment

and finds a violation of Articles 6.1.c), 6.3 and 9.2.i) of the GDPR.

II.3.4 Finding 337: Violation of the principle of transparency and the obligation

information in accordance with Articles 5.1.a., 12 and 13 of the GDPR

122. The Inspection Department notes that the persons concerned by the processing may be

divided into two categories: passengers and any accompanying persons (on departure) and people

arriving from a red zone (on arrival).

123. The methods of communicating information may also vary, since part of the information

methods of communication are used vis-à-vis all the persons concerned, whereas

³⁶ Commercial Aviation Protocol, p. 5. It is the Litigation Chamber that highlights.

³⁷ For reasons of readability and understanding of the decision, finding 3 is examined before finding 2.

Decision on the merits 47/2022 - 25/73

certain additional information is communicated only to passengers and potential

companions on departure. This information is provided via the four means of communication

following:

- An information banner published on the defendant's website;

- A "frequently asked questions" page on the defendant's website;

- The internal rules published on the site and displayed before the temperature checks

bodily injury of passengers;

- The privacy statement published on the defendant's website.

124. With regard to departures, the defendant also indicated that it had posted a poster

containing an infographic indicating a temperature above 38°C, with the mention "no access

to the terminal". The poster also shows a face in profile whose temperature is taken using

a forehead thermometer.

125. The Inspection Service finds breaches of Articles 5.1.a), 12 and 13 of the GDPR with regard to

concerns the information communicated to the persons concerned at the outset. Violations can

be distinguished according to whether they took place between June 15, 2020 and December 2, 2020 (date of the

posting of the new privacy policy) or that they are subsequent to this

last date.

126. In general, during the hearing, the defendant agreed that certain points could have been

be improved, in particular with regard to the retention period and the reference to DPA. For

the defendant, the Inspection Service adds a criterion to the GDPR by imposing to resume the base

precise legal information, but she understands that this could improve the quality of the information. The policy of

Privacy was last modified November 2020 (published December 2, 2020) on several

aspects, but it does not yet contain a reference to Article 9 of the GDPR.

127. For the defendant, the fact that there was not a single request to exercise the rights, or

of clarifications when the contact details of the DPO were available in several places is a

proof that transparency was guaranteed.

128. To the extent that the information provided to data subjects has varied over time and depending on the circumstances, the Inspection Service has chosen to examine compliance with these principles in three different situations, which are listed below.

a) Violations that occurred between June 15 and December 2, 2020 for departures

IS Findings

Decision on the merits 47/2022 - 26/73

129. With regard to the violations that took place between 15 June and 2 December 2020 for the departures, the Inspection Service considers that they relate to the following elements³⁸:

-

The fact that the temperature control is done by means of thermal cameras is not indicated in any of the means of communication (violation of Article 5.1.a);

- The legal basis of the processing is never announced (violation of Article 13.1.c), nor is the regulatory framework of the obligation to monitor body temperature (violation of Article 13.2.e));

- The retention period is not determined or the criteria used to determine these ci are not mentioned (violation of Article 13.2.a));

- The right to lodge a complaint with the DPA is also not mentioned (13.2.d)).

- The purpose of the processing is not mentioned (Article 13.1.c))

Position of the defendant

130. The defendant considers that the Inspection Service did not take into account certain documents published in order to verify compliance with its legal obligations.

131. It considers that the information concerning the taking of body temperature by means of thermal cameras was not necessary as this information was already available through the national press and an airport press release dated June 10, 2020 and that the persons concerned therefore already had this information (Article 13.4 of the GDPR).

132. Furthermore, on the basis of this same exception, the defendant considers that the persons

concerned should already be aware of the existence of the legal obligation governing the processing being
given that this results from the Protocol, itself imposed by ministerial decrees, which are
published in the Belgian Official Gazette³⁹. The defendant considers that it cannot be held liable for the
delay in publication of the Protocol.

133. With regard to the retention period, the defendant acknowledges that it should have indicated this
precisely. It also recognizes that the existence of the right to lodge a complaint
with ADP, is not included in the Privacy Policy.

134. She puts forward the same arguments as those presented with regard to Finding 2 which concerns
specifically the question of purpose (see points 187 and following below).

38 Since the privacy statement does not explicitly mention the temperature screening of the data subjects, it
has not been examined by the Inspection Service. The findings of violations therefore relate to the three other means of
communication.

39 The conclusive again insists that it cannot be held responsible for the delay in publishing the protocol.

Decision on the merits 47/2022 - 27/73

Examination by the Litigation Chamber

135. The principle of transparency is established in Article 5.1.a) of the GDPR which indicates that "the data to be
personal character must be processed in a lawful, fair and transparent manner with regard to the
data subject (lawfulness, fairness, transparency); »

136. This principle is implemented, among other things, by Article 12.1 of the GDPR, which specifies that the person responsible
processing "take appropriate measures to provide any information referred to in Articles 13
and 14 as well as to carry out any communication under Articles 15 to 22 and Article 34 in
regarding the processing to the data subject in a concise, transparent,
understandable and easily accessible, in clear and simple terms (...)".

137. Recitals 58 and 60 of the GDPR specify that "the principle of fair and transparent processing
requires that the data subject be informed of the existence of the processing operation and its
purposes" and that "the principle of transparency requires that any information sent to the public or to the

data subject is concise, easily accessible and easy to understand, and formulated in

plain and simple terms (...).".

138. As Advocate General P. Cruz Villalón and the Court of Justice of the European Union have pointed out

European Union in the Bara case, compliance with the provisions on transparency and

information is essential because it is a prerequisite for the exercise by people

concerned of their rights, which are one of the foundations of the GDPR⁴⁰.

139. In the event that the personal data concerned have been collected from the person

data subject itself, Article 13 of the GDPR specifies what information must be provided to it.

140. In its guidelines on transparency, Working Party 29 clarified that Article 13 of the

GDPR applies both where personal data is transferred

knowingly by the data subject to the controller and in cases where

the data is collected by the data controller by observation (for example by

the use of automated data collection equipment or data capture software

data such as cameras).⁴¹

141. With regard to the first element, i.e. processing on the basis of cameras

heat, the Litigation Chamber finds that the defendant claims the application

of Article 13.4 of the GDPR and indicates that it was not subject to the obligation to inform the persons

concerned since they already had the information through the media and a

Airport press release.

⁴⁰ CJEU, 1 October 2015, Bara, C-201/14, par. 33 (Conclusions of Advocate General P. Cruz Villalón, July 9, 2015, par. 74).

⁴¹ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 11 April 2018, p. 14-15, by 26.

Decision on the merits 47/2022 - 28/73

142. Article 13.4 of the GDPR makes it clear that paragraphs 1, 2, 3 do not apply where, and

insofar as the data subject already has this information. Article 13.4 does not

therefore does not constitute an exception to the principle of transparency as formulated in Article 5.1.a of the

GDPR. However, it was indeed on the basis of this article that the Inspection Service noted a breach of

the obligation to inform the persons concerned of the existence of thermal cameras. For the Litigation Chamber, a distinction must indeed be made between the principle of loyalty and of transparency on the one hand (Article 5.1.a) and the obligations arising from this principle (in particular the sections 13 and 14).

143. The principle of fairness and transparency established in Article 5.1(a) is not limited to simple information and transparency obligations listed in the articles of the GDPR, but consists of a general principle, the scope and philosophy of which must be respected for any treatment.

144. This point of view was formally adopted by the EDPS in his decision 01/021 concerning Whatsapp, in which he indicates that:

“Based on the above considerations, the EDPB emphasizes that the principle of transparency is not not circumscribed by the obligations arising from Articles 12 to 14 of the GDPR, although the latter are a concretization of the first. Indeed, the principle of transparency is a general principle which not only reinforces other principles (e.g. fairness, accountability), but whose stem from many other provisions of the GDPR. Furthermore, as indicated above, the article 83(5) of the GDPR provides for the possibility of finding a violation of the transparency obligations regardless of the violation of the principle of transparency. Thus, the GDPR distinguishes the dimension of the principle of more specific obligations. In other words, the obligations of transparency do not define the full scope of the principle of transparency. »⁴²

145. It is therefore right that the Inspection Service bases itself on the principle of transparency of Article 5.1.a) to consider that the persons concerned should have been informed of the existence of the thermal cameras, although this obligation is not expressly found in the obligations of transparency of article 13 of the GDPR.

146. However, recital 60 of the GDPR indicates that “The principle of fair and transparent processing requires that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any other information necessary to ensure fair and transparent processing, taking into account the

particular circumstances and the context in which the personal data is

processed".

42 EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Whats

Ireland under Article 65(1)(a) GDPR, 28 July 2021, §192. Free translation.

Decision on the merits 47/2022 - 29/73

147. The fact that the temperature is taken by means of thermal cameras is an element

important for data subjects to be informed about the processing of their data. In

Indeed, the principle of fairness and transparency of Article 5.1.a) requires by its essence that the

data subjects know when their data is being processed or not.

148. The Litigation Chamber finds that during the period examined, the control of the temperature

was mentioned in two different documents provided by the defendant: the Rules of Order

Interior (hereafter: ROI) and the FAQ page which was accessible via the banner on the website. None

of these two sources of information does not mention that the processing would or could be carried out

using thermal cameras.

149. As the defendant points out, the fact that thermal cameras are used at the airport

is information that was repeated in several press articles. For the Litigation Chamber,

the defendant cannot, however, rely sufficiently on the existence of information in

the press to dispense with its obligations of transparency with regard to the GDPR and with regard to

persons concerned. Indeed, it cannot be presumed that any passenger in transit at the airport

has read a press article allowing them to be fully informed of the existence and conditions of the

treatment. In addition, data controllers cannot transfer their responsibility by

matter of transparency to the press and must assume them personally and directly.

150. The use of thermal cameras was also made public by the defendant in

a press release published on June 10, 2020 on its website. If this initiative is in itself

commendable, it is insufficient for the Litigation Chamber. Indeed, the principle of transparency

requires that information be accessible in a centralized and consolidated way, for example through the

ROI or privacy policy, which are easily accessible⁴³. A press release,□

which must, after a certain period, be the subject of a search in the web archives of a manager□

treatment cannot be described as “easily accessible”.□

151. Furthermore, the Litigation Chamber finds that the poster affixed by the defendant (see□

point 124) indicates that the temperature is taken using a manual forehead thermometer,□

while the first temperature is taken using thermal cameras.□

152. In view of the elements presented above, the Litigation Chamber considers that the persons□

concerned were not properly informed that their temperature might be taken□

by thermal cameras and that it would therefore have been possible that the temperature of a person□

concerned is taken without his knowledge□

The Litigation Chamber therefore finds a violation of Article 5.1.a) of the GDPR.□

43 Recital 58: “[...] The principle of transparency requires that any information sent to the public or to the data subject be□

concise, easily accessible and easy to understand, and stated in clear and simple terms and, in addition, where appropriate, illus□

using visual elements [...]”.□

Decision on the merits 47/2022 - 30/73□

153. The second element to be examined concerns information about the legal basis of the processing□

(article 13.1.c), and the regulatory framework of the obligation to monitor body temperature (article□

13.2.e)). The Inspection Service found that this information was not available in any of the□

sources of information available to data subjects. In this regard, the defendant□

claims the applicability of Article 13.4, indicating that the persons concerned could not□

ignoring the existence of this obligation, since it is based on the Protocol, expressly provided□

by ministerial decrees published in the Belgian Official Gazette.□

154. The Litigation Division cannot accept this argument put forward by the defendant. This□

would imply that controllers should never inform individuals□

concerned of the legal basis of the processing as soon as this has been published in the Belgian Official Gazette.□

This logic obviously goes against Articles 13.1c), 13.2.e) and recital 58 which□

require that this information be provided in a manner that "is concise, easily accessible and easily to understand, and formulated in clear and simple terms."

155. Furthermore, the exception provided for in Article 13.4 only applies "where and to the extent that the data subject already has this information", which implies that the data subject must actually have this information. The mere fact that the information is available at the Belgian Monitor does not meet this criterion. In any case, the Protocol on which the defendant to base the disputed processing had not even made the obligation of a publication before mid-August 2020, when it was supposed to apply from 8 June⁴⁵.

156. In addition, contrary to what the defendant claims, the data controller must firstly inform the data subject on which paragraph of Article 6 the data processing is based and, in another time, what is the text and the precise provision which bases the legal obligation on which would be based on the processing carried out under Article 6.1.c) of the GDPR. A pure reference to an "obligation legal" without reference to the latter cannot be sufficient for the information of the persons concerned is considered sufficient. The persons concerned could not, in these circumstances, never verify whether a legal obligation within the meaning of Article 6.1.c actually exists and derives from the legal provision in question.

157. The Chamber finds that this is not the case here since the Respondent did not reference neither to the Protocol in question nor to the ministerial decrees at the time of the implementation of the processing as the basis of its legal obligation to base the processing. By moreover, the data processed being health data, the defendant must be able to justify a exceptions provided for in Article 9.2 of the GDPR, which must be reflected in the information provided to the concerned person. This reference to specific legal norms is essential for the

44 GDPR, recital 58.

45 Investigation report, p. 32. The Inspection Service points out that this publication by the FPS only took place following its inte in another similar folder.

Decision on the merits 47/2022 - 31/73

data subject can be aware of the rights available to him and the obligations

to which it is subject for each treatment.

158. The Litigation Chamber therefore finds a violation of Articles 13.1c) and 13.2.e) of the GDPR.

159. With regard to the third and fourth element, i.e. the retention period of the

data, and the right to lodge a complaint with a data protection authority, the

Litigation Chamber finds that these breaches are admitted by the defendant. The violation

of Articles 13.2.a) and 13.2.d) is established.

160. With regard to the fifth question, which is that of purpose, the Litigation Chamber

refers to these considerations below, in which it believes that the purpose was not

sufficiently explained in the information documents, before the modification of the policy

of confidentiality on December 2, 2020 (point 195 et seq.). It therefore finds a violation of Article

13.1c) on this point.

161. The Litigation Chamber therefore finds a violation of Articles 5.1.a, 13.1c), 13.2.d, 13.2.a, and

13.2.e) between June 15 and December 2, 2020 for departures.

b) violations that occurred on or after December 2, 2020 for departures

Findings of the Inspection Service

162. With regard to the violations which had from 2 December 2020 for departures⁴⁶, the

Inspection Service considers that they relate to the following elements:

- The basis of lawfulness invoked is not sufficiently precise (violation of Article 13.1.c));

- The fact that the temperature control is done through thermal cameras is never

stated (violation of Article 5.1(a));

- The possible consequences of non-provision of data are not indicated any more

that there is no reference to the ROI (violation of Article 13.2.e));

- Insufficiently precise mention of the purpose of the processing (see points 184 et seq.);

- The privacy notice always refers to the law of 8 December 1992 which has been repealed.

Position of the defendant

163. The defendant considers that the amendment to its privacy notice (dated November 23 2020, published December 2, 2020) clearly indicates the basis of legality. She believes that the 46 Date on which the amended privacy statement was posted.

Decision on the merits 47/2022 - 32/73

Inspection Service adds a condition to Article 13.1.c requiring that the provision(s) legal basis for the processing is clearly cited.

164. Regarding the lack of information on the use of cameras, as well as the question of the purpose, the defendant refers to its considerations above (see point 141 et seq. and 160) and dispute the grievances.

165. Regarding the reference to the ROI, she believes that this could indeed have been done better, but this does not in itself constitute a breach of its duty to inform, especially since the ROI is present inside the enclosure before any temperature control.

166. The defendant acknowledges a material error as to the reference to the law of 1992 which will be corrected.

Position of the Litigation Chamber

167. The first element concerns compliance with Article 13.1.c) which requires mention of the legal basis of the treatment. As indicated both by the Inspection Service and by the defendant, from of December 2, 2020, the defendant's privacy policy contained the statement next :

168. "When we are in times of epidemic or pandemic, we are likely to take the temperature to check if it is above 38°C. This temperature measurement is only done on the basis of a legal obligation and this data is not stored or reused at purposes other than to ensure the health security of persons passing through the airport. The duration conservation is a few minutes. »

169. The defendant considers that this meets the requirements of Article 13.1c) of the GDPR while the Inspection Service considers that the specific legal provision(s) should have been included,

same as the exception listed in article 9.2 of the GDPR allowing it to justify the processing of health data.

170. For the Litigation Division, compliance with Article 13.1.c) implies that the person concerned must to be informed in an exhaustive manner both of the precise basis of lawfulness on which the processing is based but also of the text and the precise provision of the latter which creates the legal obligation which bases the processing under Article 6.1.c). It refers on this subject to points 153 et seq. above and finds a violation of Article 13.1.c) of the GDPR.

171. The second question relates to the fact that the temperature control is done through thermal cameras would never be indicated (violation of article 5.1.a)). The Litigation Chamber Decision on the merits 47/2022 - 33/73

refers on this subject to its position expressed above and which remains valid in the present case (see paragraphs 141 and s.) and finds a violation of Article 5.1.a) of the GDPR.

172. The third question relates to the absence of any mention of the possible consequences of not provision of the data due to the absence of reference to the ROI (violation of Article 13.2.e)). the Inspection Service considers that the obligation to indicate the regulatory nature of the obligation to provide the data and the possible consequences of not providing the character data personnel, which are a requirement set out in Article 13.2.e) of the GDPR are not met. The defendant considers that, since this information is in the ROI, Article 13.2.e) is complied with, although a reference to ROI could have been made in the privacy policy.

173. The Litigation Chamber notes discrepancies between the information provided to persons concerned according to the document examined. Indeed, the privacy policy mentions that the processing is based on a legal obligation (even if this statement is incomplete, see point 153 and s.). On the other hand, it does not mention at any time the consequences of a refusal of treatment. As far as the ROI is concerned, it clearly mentions that access to the terminal will be refused "to any person refusing to submit to temperature screening or whose body temperature is above 38°C after at least two readings"⁴⁷. On the other hand, it does not indicate the source of this

obligation.⁴⁸ The same is true for the “Frequently Asked Questions (FAQ)” page, which indicates ☐ the consequences of a temperature above 38°C, but not the source of this obligation. ☐ None of these three documents refers to the other, which implies that a data subject ☐ who would have consulted only one document would not have had all the information available to them. ☐ was entitled to receive. For the Litigation Chamber, this contravenes the requirements of a ☐ information "concise, easily accessible and easy to understand, and formulated in clear terms ☐ and simple"⁴⁹. It therefore finds a violation of Article 13.2.e) of the GDPR. ☐

174. The fourth question relates to the mention of the purpose. On this point, the Litigation Chamber ☐ notes that from December 2, 2020, the purpose was explained in the privacy policy ☐ of the defendant in the form of "ensuring the health security of people passing through ☐ the airport". However, this purpose is not found as such in the ROI. ☐

175. The fifth question relates to the reference to the law of 8 December 1992 (which has been repealed) in the ☐ privacy policy. This element is not disputed by the Respondent and the Chamber. ☐ litigation therefore finds that this statement is inaccurate and must be updated. ☐

176. The Litigation Division therefore finds a violation of Articles 5.1.a, 13.1c) and 13.2.e). ☐

47 ROI, Article 8 and FAQ ☐

48 ROI, Article 8: “The airport is under an obligation”. ☐

49 GDPR, recital 58. ☐

Decision on the merits 47/2022 - 34/73 ☐

c) Arrivals from a red zone ☐

Findings of the Inspection Service ☐

177. With regard to arrivals from a red zone, the Inspection Service found a violation ☐

Articles 5.1a, 12.1 and 13 of the GDPR based on the elements below: ☐

- The information contained in the ROI and on the website indicates that the purpose of these ☐ controls is to limit access to the terminal to people with a higher temperature ☐ at 38°C, which in the context of checks on arrivals is incorrect (see point 49); ☐

- The fact of not mentioning at any time that the temperature control is done by means of

thermal cameras;

- The fact that the information communicated to passengers returning from the red zone does not reflect

the conditions under which the control is carried out (article 5.1.a).

Position of the defendant

178. The defendant considers first of all that the initial premise of the Inspection Service is incorrect,

since he considers that he is wrongly limiting himself to only two documents when he should have considered

all sources of information.

179. She adds that only a version of the ROI has been put online for reasons of economy and efficiency. By

elsewhere, the ROI clearly states that passengers' temperatures will be taken.

180. Finally, the defendant challenges the innovative nature of thermal cameras.

Position of the Litigation Chamber

181. On the first question, which concerns the purpose of taking the temperature, the Litigation Chamber

indeed notes that the ROI mentions that temperature control is compulsory and that the

people who refuse to submit to it or who have a temperature above 38°C after

at least two controls will be refused access to the terminal. The ROI does not mention the case of

returns from the red zone, or the only consequence of a temperature above 38°C is that the

person concerned is given an awareness document. Delivery of this document is

without major consequences for the rights of the data subject. However, by not specifying

that the control described only applies to departures, the text of the ROI implies that a person

could be refused access to the terminal upon arrival, which creates confusion and poses a problem

with regard to the principle of transparency.

Decision on the merits 47/2022 - 35/73

182. With regard to the wording of the information banner and the "Frequently Asked Questions"

questions (FAQ)" published, these do not specify either that the prohibition of access to the terminal does not

applies only to departures, which could lead the persons concerned to think that they can

be denied access to the terminal upon arrival as well. This again poses a problem for

with regard to the principle of transparency (article 5.1.a) of the GDPR).

183. On the second question, the Chamber refers to its considerations above, which remain valid.

It also notes that, as pointed out by the Inspection Service, the posters which were

affixed to departures (see point 124), are not present at arrivals, which implies that

the information available to passengers arriving from a red zone is even more incomplete than that

provided to departing passengers.

184. The Litigation Chamber therefore finds a violation of Articles 5.1.a), and 12.1.

II.3.5 Finding 250: Violation of the principle of limitation of the purpose of the data

in accordance with Article 5.1.b. GDPR

Findings of the Inspection Service

185. The Inspection Service considers that the purpose of the processing is the “health safety of

people transiting through the airport and employees working in the terminal”, since this is the

answer given to it by the defendant during the investigation and which recalled in the Analysis

of impact relating to the protection of personal data that the defendant transmitted

to the Inspection Service

186. The Inspection Service notes that the defendant did not determine with sufficient

specifies the purpose of the processing concerned in accordance with article 5.1.b of the GDPR in the sense

or the data controller has not specified that the processing has a different objective and relates to

different consequences for the persons concerned depending on the type of control

made (on departure or on arrival).

Position of the defendant

187. The defendant recalls first of all that the notion of purpose is not defined in the GDPR and

that it is therefore based on a definition of the CNIL. It considers that the purpose of the processing is

sufficiently determined: the aim is to ensure the health security of people passing through

the airport and employees in the terminal. The definition of the consequences of a treatment is not

50 As previously indicated, the Litigation Division decided to reverse the examination of findings 2 and 3 of the Report of investigation.

Decision on the merits 47/2022 - 36/73

a condition of regulatory validity of the purpose limitation principle. The defendant adds that the difference in treatment between departures and arrivals was justified by their situations distinct and follows from common sense. People arriving from a red zone cannot be sent home. She adds that she has never had to refuse access to the entrance to the terminal to people concerned whose temperature was above 38°C, since they have decided in full thank you for not continuing on their way.

188. She concludes that the purposes of the processing were clear, defined and legitimate and that she has always complied with the principle of proportionality by balancing the health interests of public and the privacy of the persons concerned.

Examination by the Litigation Chamber

189. Article 5.1.b of the GDPR specifies that the data must be processed for specified purposes, explicit and legitimate. For the Litigation Chamber, in the present case, the question of the finality of the treatment announced by the defendant can be analyzed separately from the question the purpose stated in the legal basis (see points 102 and following above). The legal basis invoked does not specify the purpose or does not specify it sufficiently clearly (see points 195 and s.). It is therefore necessary to examine the purpose announced by the data controller.

190. For the interpretation of this principle, the Litigation Chamber refers to the opinion of the Working Group Article 29, which details what is meant by an explicit purpose⁵¹ under Directive 95/46⁵².

It is important to note that the main features of the purpose limitation principle have remained identical between Directive 95/46⁵³ and the GDPR.

191. Regarding the determined nature of the purpose, the Litigation Chamber notes that this purpose is clearly indicated by the defending party in its response to questions from the Service inspection as being “the health security of people transiting through the airport” and is by

the follow-up recalled in the Impact Assessment relating to data protection carried out by the party

defendant. It is also indicated in a shortened form in the Register of

processing activities in the form of “health security”.

192. The Litigation Chamber therefore considers that the purpose is sufficiently determined.

51 “ARTICLE 29” Working Party on Data Protection, “Opinion 03/2013 on purpose limitation”, op. cit., p. 17. Translation free.

52 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons at with regard to the processing of personal data and the free movement of such data

53 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons at with regard to the processing of personal data and the free movement of such data

193. Regarding the explicit nature of the purpose, the opinion of the Article 29 Working Party explains this

Decision on the merits 47/2022 - 37/73

following :

"The purposes of the collection must not only be specified in the minds of the people responsible for data collection. They must also be explained. [...]"

The ultimate objective of this requirement is to ensure that the objectives are specified unambiguously or vagueness as to their meaning or intent. The meaning must be clear and must not leave no doubt or difficulty in understanding. [...]"

The obligation to specify the objectives "explicitly" contributes to transparency and predictability.

It makes it possible to unambiguously determine the limits of the use that those responsible for the processing may make personal data collected, with a view to protecting the

persons concerned. It helps anyone who processes data on behalf of the data controller

processing, as well as data subjects, data protection authorities and other

stakeholders, to have a common understanding of how data can be

used. This reduces the risk that the expectations of the people concerned differ from

those of the data controller”⁵⁴.

194. The opinion of the working group therefore insists on the need for an explanation of the purpose that allows anyone to understand the purpose of the data processing and to avoid the misunderstandings. Regarding the way in which this purpose should be explained, the opinion underlines the following elements:

"In terms of responsibility, the specification of the objective in writing and the production of documents adequate will help demonstrate that the controller has complied with the requirement of

Article 6(1)(b). This would also allow data subjects to exercise their rights more effectively - for example, this would provide evidence of the original purpose and would allow a comparison with the subsequent processing purposes. »⁵⁶

195. The Litigation Chamber considers that this point is therefore closely linked to the question of the transparency and information. As such, it refers to the observations made above (see point 162 and 174), which she also completes here. It appears from the various sources of documentation that

54 "ARTICLE 29" Working Party on Data Protection, "Opinion 03/2013 on purpose limitation", op. cit., p. 17. Translation free.

55 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

56 "ARTICLE 29" Working Party on Data Protection, "Opinion 03/2013 on purpose limitation", op. cit., p. 18. Translation free.

Decision on the merits 47/2022 - 38/73

the privacy policy did not contain any information about the purpose of the processing before its modification on December 2, 2020. It was only during this modification that the purpose was added, drafted in the following form: "ensure the health security of people transiting through the airport".

196. The ROI did contain an article 8 indicating that access to the terminal will be refused "to any person refusing to submit to temperature screening or whose body temperature is above 38°C after at least two readings". The purpose can be deduced from the text of the ROI, but

it is not clearly explained or linked to a particular treatment. The FAQ page contains

also a similar sentence.

197. In view of the above elements, the Litigation Division concludes that the purpose of the processing was not

not explicit. Not only was it not announced when the treatment was set up,

but it was only following an answer to a question from the Inspection Service, the modification of the

privacy policy in December 2020 and at the completion of the DPIA, three months after the start

processing that this purpose was articulated, explicitly formulated and communicated to the DPA as well as

only to the persons concerned.

198. As to the legitimacy of the purpose, the Litigation Chamber considers that the purpose "to ensure the

health security of people transiting through the airport and employees working in the

terminal" is quite legitimate, particularly in view of the fact that the processing has been recognized as

justified by reasons of public interest in the field of public health in accordance with Article

9.2.i. of the GDPR (see point 84)

199. The Litigation Division therefore finds a violation of Article 5.1.b) of the GDPR due to the

non-explicit nature of the purpose.

II.3.6 Finding 4: violation of the obligation to carry out an impact study relating to the

data protection prior to processing (violation of Article 35.1.)

200. Based on its investigation, the Inspection Service comes to the conclusion that Article 35.1 of the GDPR has

been violated, due to the items below.

a) On the obligation to carry out a DPIA

Findings of the Inspection Service

201. The Inspection Service considers that a DPIA was necessary on the basis of the following criteria:

Decision on the merits 47/2022 - 39/73

- The processing concerns sensitive data, namely data concerning health;

-

This is a large-scale treatment;

- The processing involves systematic monitoring of certain passengers via the submission□

mandatory body temperature check;□

- The processing includes an innovative use or application of new technologies□

or organizational;□

- The processing concerns, in part, vulnerable people and in particular□

minors;□

- Article 23 of the law of 30 July 2018⁵⁷ explicitly provides that “in execution of article□

35.10 of the Regulation, a specific data protection impact analysis is□

carried out before the processing activity, even if a general impact analysis relating to the□

data protection has already been carried out in the context of the adoption of the legal basis. ”.□

Position of the defendant□

202. The defendant specifies first of all that only the data of people whose temperature is□

above 38°C are processed, since only these are the subject of an image taken by camera.□

203. Regarding the notion of large scale, the defendant considers that the Inspection Service does not□

not based on the right figures, since it takes into consideration all the people who have□

transited through the airport and not people who had a temperature above 38°C. He is at□

it is currently impossible to know this number of people since the summary files□

number of interventions were destroyed each week.□

204. In addition, with regard to passengers returning from the red zone, the Inspection Service□

would consider, without any reason, that it is a large-scale treatment.□

205. The defendant considers that only the criterion of systematic surveillance of certain passengers□

is relevant in the present case. It was this criterion alone that forced him to undertake a DPIA.□

206. Finally, the defendant disputes the innovative nature of the cameras, which are old technology□

according to her.□

Examination by the Litigation Chamber□

207. Article 35 specifies the circumstances in which it is necessary for a person responsible for□

processing to carry out a DPIA. This article is reproduced in part below:□

57 Law of 30 July 2018 on the protection of individuals with regard to the processing of personal data.□

Decision on the merits 47/2022 - 40/73□

“Rule 35□

Data Protection Impact Assessment□

1. Where a type of processing, in particular through the use of new technologies, and account□

given the nature, scope, context and purposes of the processing, is likely to generate□

a high risk to the rights and freedoms of natural persons, the controller□

carry out, before the processing, an analysis of the impact of the planned processing operations on the□

protection of personal data. One and the same analysis can relate to a□

set of similar processing operations that present similar high risks.□

2. When carrying out a data protection impact assessment, the data protection officer□

processing shall seek advice from the data protection officer, if such a officer has been appointed.□

3. The data protection impact assessment referred to in paragraph 1 shall, in particular,□

required in the following cases:□

has)□

the systematic and in-depth evaluation of personal aspects concerning people□

physical, which is based on automated processing, including profiling, and on the basis of□

which are taken decisions producing legal effects with regard to a person□

physical or significantly affecting it in a similar way;□

b)□

the large-scale processing of special categories of data referred to in Article 9,□

paragraph 1, or personal data relating to criminal convictions and□

offenses referred to in Article 10; Where□

vs)□

systematic large-scale monitoring of an area accessible to the public. »□

208. The Litigation Division also specifies that the DPA has adopted a list of processing operations for which a DPIA is required⁵⁸. She also notes that with regard to the use of cameras and thermal data, the European Data Protection Supervisor (EDPS) has already been able to confirm in a position paper dated February 1, 2015 that the completion of a DPIA is indeed required⁵⁹.

209. Furthermore, the Litigation Division considers that recital 91 of the GDPR corroborates the need to carry out a DPIA in this situation, since it indicates in particular that “An analysis of the impact assessment relating to data protection should also be carried out when data of the of protection

58 Authority

January

<https://www.autoriteprotectiondonnees.be/publications/decision-n-01-2019-du-16-janvier-2019.pdf>

59 EDPS, Letter from

01_letter_klimowski_2015_en.pdf

February 2015. Available at:

Data, Decision

2019

#01

from

16

1st

<https://edps.europa.eu/sites/default/files/publication/16-02->

2020. Available

on :

Decision on the merits 47/2022 - 41/73

of a personal nature are processed for the purpose of making decisions relating to persons

specific physical features following a systematic and thorough assessment of personal aspects

specific to natural persons on the basis of the profiling of said data or following the

processing of special categories of personal data, data

biometrics or data relating to criminal convictions and offences, or to

related security measures".⁶⁰

210.

It has been established that the processing in question relates to special categories of data

(health data) and that it has the consequence, in any case for the processing taking place at the

departures, to decide whether or not passengers and accompanying persons can enter the terminal.

211. The Litigation Chamber notes that the defendant does not dispute the fact that a DPIA

was mandatory for the processing in question. His criticisms relate essentially to the criteria

retained by the Inspection Service, the relevance of which it sometimes contests (points 202-206 below).

above) .

212. For the Litigation Chamber, the defendant makes a retrospective and erroneous assessment

criteria for determining whether a DPIA is required. Indeed, when the party

defendant had to carry out its DPIA (see points 261 et seq. below) it was unaware of the percentage

passengers who would have a temperature above 38°C and therefore could not at this stage

determine that he was "extremely weak", as she does a posteriori in her conclusions⁶¹.

The defendant should have considered that all

expected passengers could

potentially be a data subject. It is therefore this figure that should be taken into account.

consideration to judge whether it was a large-scale treatment or not.

213. Moreover, although the temporarily stored images only concern people with a

temperature above 38°C, it is indeed all the passengers and accompanying persons at the

departure and all passengers returning from the red zone who are subject to verification of the

temperature. The IS therefore relies on correct reasoning by determining that to determine

“the nature, scope, context” of the processing, it had to be considered that it applied to

all the passengers concerned and not only those whose temperature was higher than

38°C.

214. As for the innovative nature of thermal cameras, the Litigation Chamber considers that this

criterion, assuming that it is not established, does not change the conclusion that follows, namely that a DPIA

was needed.

215. The Inspection Service also considered that a DPIA was required under article 23 of the law

of July 30, 2018 (see point 201), which specifies that “a specific impact analysis of the protection of

60 It is the Litigation Chamber which highlights.

61 Defendant's submissions, p. 45

Decision on the merits 47/2022 - 42/73

data is carried out before the processing activity, even if a general impact analysis relating

to data protection has already been carried out in the context of the adoption of the legal basis”. The

Litigation Chamber points out, however, that this article only applies to the public sector,

as specified in Article 19 of the same law and is therefore not applicable in this case.

b) On the obligation to carry out a DPIA prior to processing

Findings of the Inspection Service

216. The Inspection Department notes that the DPIA of BSCA S.A. was carried out on 18 September 2020 whereas

that the processing operations concerned were implemented on June 15, 2020 concerning the persons

concerned on departure and on 7 September 2020 for passengers returning from a red zone. According

the Inspection Service, the DPIA must be carried out prior to the implementation of the processing and

no exception is provided for by Article 35 of the GDPR.

Position of the defendant

217. The defendant emphasizes the exceptional nature of the situation in which it found itself. If he

is true that no exception exists to this obligation in the GDPR, the defendant

considers that this is clearly a case of force majeure which could not have been foreseen by the legislator.□

She indicates that the DPD had been laid off, like the majority of his staff.□

It was only when the health situation calmed down that the defendant was able to carry out the DPIA, at□

posterior. She also recalls that she had no choice but to set up the system of□

control and that although this does not release it from its obligation, it carried out this one as soon as it□

been able to do that.□

Examination by the Litigation Chamber□

218. For the Litigation Division, it is clear from the text of the GDPR⁶², as admitted by the part□

defendant that the DPIA must be carried out before the implementation of the processing. The text does not provide□

no exceptions. The Litigation Chamber notes that the DPIA was only carried out on September 18□

2020, i.e. three months after the start of the treatment (June 15, 2020).□

219. The defendant does not demonstrate how the conditions for such force majeure would have existed.□

220. The Litigation Chamber therefore finds a violation of Article 35.1 of the GDPR.□

⁶² GDPR, article 35.1° and recital 90.□

Decision on the merits 47/2022 - 43/73□

c) On the quality of the DPIA carried out by the defendant in accordance with Article 35.7 of the GDPR□

On the description of the processing operations and the purposes of the processing of the DPIA (article□

35.7.a GDPR)□

Findings of the Inspection Service□

221. The Inspection Service notes, as indicated above (see point 186), that the□

purpose of the processing is not sufficiently specified.□

222. It also considers that the DPIA does not describe, in a sufficiently precise manner, the procedure□

in place surrounding passenger body temperature screening and more specifically□

concerning the consequences that such a control could have for the persons concerned.□

223. In addition, the Inspection Service considers that the DPIA contains certain inconsistencies, in particular□

re□

recording/retention of personal data□

coming from the cameras□

nor does it highlight the analysis as to the quality of the legal basis□

invoked in accordance with Articles 6.1., 6.3. and 9.2.i. of the GDPR.□

Position of the defendant□

224. In general, the defendant is surprised by certain criticisms leveled at it, given□

that it referred to the CNIL model to carry out its DPIA, since the DPA does not have any□

tool about it.□

225. The defendant recalls that there is no definition of the concept of purpose in the GDPR and that it□

has chosen to define it as follows: “the health security of people transiting through□

the airport and employees working in the terminal”. The defendant considers that this definition□

is very clear.□

226. As regards the type of procedure employed, the defendant considers that this is left to the□

discretion of the data controller and that several methodologies exist. The□

defendant argues that it is difficult to conceive that the use of a tool from a□

another authority leads to a finding of breach even though the DPA does not provide a tool to□

arrangement.□

227. The defendant adds that the consequences for the persons concerned are well known to the□

data controller – and data subjects with regard to the information provided to them□

Decision on the merits 47/2022 - 44/73□

provided – and therefore it is not, per se, necessary to state every consequence in the DPIA as long as□

the final result indicates the risks for the rights and freedoms of the data subjects.□

228. Regarding the inaccuracies mentioned, the defendant argues that□

the DPIA contains□

all the information relating to the processing with an explanation as to the fact that the□

software keeps the last 20 images and that this information is in the AIPD at various□

points. It therefore considers that this information is not lacking, since it is mentioned

in other places in the DPIA.

229. With regard to the legal basis, the defendant considers that it is not for the IS to reproach a

data controller potential shortcomings of the executive responsible for applying the laws and

put in place implementing decrees for these laws.

Examination by the Litigation Chamber

230. Article 35.7 contains an enumeration of the elements that a DPIA must contain. It is reproduced below

below:

“7. The analysis shall contain at least:

a) a systematic description of the processing operations envisaged and the purposes of the

processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations with regard to

purposes;

c) an assessment of the risks to the rights and freedoms of data subjects in accordance with

in paragraph 1; and

d)

the measures envisaged to deal with the risks, including guarantees, measures and

security mechanisms aimed at ensuring the protection of personal data and

provide proof of compliance with these regulations, taking into account the rights and interests

legitimate interests of data subjects and other affected persons. »

231. With regard to the purpose of the processing, the Litigation Division refers to the considerations

above (see points 189 et seq.) and considers that the purpose identified by the defendant

is determined and legitimate. In the context of the DPIA, it can be considered sufficiently

described.

232. With regard to the description of the procedure put in place for taking the temperature

passages, the Litigation Division cannot subscribe to the defendant's argument

complainant of the lack of guidance from the DPA which would oblige him to use the tool provided by a
other authority. The Litigation Chamber recalls that at the beginning of 2018,
ODA

published a

Decision on the merits 47/2022 - 45/73

recommendation on DPIA63. Furthermore, the Litigation Chamber considers that a manager of
processing cannot rely on a lack of guidance from a supervisory authority
since this would be contrary to the liability principle of Article 24 of the GDPR. He is quite
free for a data controller to use tools made available to the public by
supervisory authorities of other member states of the European Union. This use is, however, left
at the discretion of the data controller who must ensure that the tool used complies with the
prescribed by the supervisory authority to which it is subject.

233. This recommendation contains in particular the following paragraph:

“Among other elements relevant to determining the nature, scope and context of
processing, we can cite: the categories of persons concerned, the scale of the processing of
data, the origin of the data, the relationship between the controller and the persons
concerned, the possible consequences for the persons concerned and the degree of ease
with which the persons concerned can be identified.

234. In this case, the DPA had indicated as early as 2018 that the DPIA should contain a description of the
possible consequences for the persons concerned. This is all the more important in the
current file since the consequences for the persons concerned were the objective of this
treatment, namely preventing people with a temperature above 38°C from entering
in the terminal and take their flight. Since this objective is the very reason for the processing, it does not
could be concealed in the description of the processing under the DPIA.

235. With regard to the mention of the data retention period, the Litigation Chamber
indeed notes that the DPIA drawn up by the defendant mentions both "no

storage of data locally on the PC, nor on paper “65,” the captured images are not

recorded. This is real-time monitoring”⁶⁶ whereas the procedure provides that the 20

latest images are available⁶⁷. For the Litigation Chamber, this lack of consistency affects

the clarity of the description of the processing operations.

236. Finally, with regard to the quality of the legal basis, the Litigation Chamber considers that it

it is up to the data controller, within the framework of the DPIA, to assess the impact of the choices

concerning the processing that has been carried out on the legal basis or, in the event of an incomplete legal basis,

describe the treatment methods that have been chosen (as well as their reasons) in order to meet

⁶³ Data Protection Authority, Recommendation No. 01/2018 of 28

<https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf>

⁶⁴ Ibid, p. 17.

⁶⁵ Respondent’s Data Protection Impact Assessment, p. 4.

⁶⁶ Ibid, p. 5.

⁶⁷ Ibid, p. 3 and 7.

February 2018. Available at

Decision on the merits 47/2022 - 46/73

breaches of the legal basis. This is all the more the case here, since the

defendant recognized the vagueness of the Protocol and the fact that a law would have been preferable⁶⁸.

237. Based on the above considerations, the Litigation Chamber finds a violation of Article

35.7.a) GDPR.

On the assessment of the necessity and the proportionality of the processing operations with regard to the

purposes ((article 35.7.b) of the GDPR)

Findings of the Inspection Service

238. The Inspection Service notes that, insofar as the purpose of processing has not been

correctly determined within the meaning of Article 5.1.b) of the GDPR, the exercise of assessing the need

and proportionality of the measure cannot be considered to have been properly

carried out.□

239. The Inspection Service also notes that the analysis is rather summary or even incorrect□
concerning the retention of personal data and that the analysis of the necessity and□
proportionality of the processing was simply limited to assessing how the collection of the□
body temperature is limited, adequate and relevant to the purpose, whereas it would have□
had to take into account the number as well as the locations of the cameras installed in order to□
collect the body temperature of the persons concerned, the permanent nature or not of the□
processing concerned, the categories of persons concerned by the collection.□

240. The Inspection Service adds that the adequacy and limited nature of the personal data□
as well as the relevance of the collection of these categories of data are not proven.□

Position of the defendant□

241. The defendant regrets that the DPA did not set up a more comprehensive tool than that of the CNIL□
to indicate the information that would be missing according to the IS. She notes that she must□
complete this tool because the elements that the inspection service mentions are not requested,□
sensu stricto, within the framework of the CNIL tool.□

242. She reiterated her criticisms already formulated indicating that, unless she is mistaken, neither the DPA nor she has any□
in-house scientific competence to analyze the relevance of temperature collection□
bodily as a potential indicator of a person's infection with the coronavirus.□

68 See paragraph 79.□

Decision on the merits 47/2022 - 47/73□

243. She adds that it is not appropriate to carry out, a posteriori, a scientific analysis of this□
need. The choice of this way of working was made by the concluding party on the basis of a□
pragmatic analysis of the possibilities which were his and, as already stated, of the practices□
used at 65 other airports around the world.□

244. She insisted on the fact that it is not the responsibility of the Inspection Service to validate or not the choice of a□
methodology in order to achieve the health safety objective pursued by the conclusive.□

Examination by the Litigation Chamber□

245. The Litigation Division has already considered that the purpose expressed by the defendant was□
sufficiently determined within the meaning of Article 5.1.b) of the GDPR (points 189 and following). So she can□
be validly used as a starting point to assess the necessity and proportionality of the□
treatment.□

246. However, for the Litigation Division, the analysis of the relevance, adequacy and character□
limited data collected is insufficient. Indeed, it is limited to a few lines which do not□
in no way demonstrate an in-depth analysis of the necessity and proportionality of the operations□
treatment. As previously indicated, the information is also inaccurate with regard to□
relates to the retention period of the data. The examination carried out by the defendant does not□
mentions that□
the data of□
the temperature and never examines□
the question□

recording an image of the data subject. However, it is in itself quite possible to□
measure people's temperature without photographing them. The purpose of the DPIA□
being precisely to assess the impact of the choices made regarding the processing methods.□

247. Moreover, as the Inspection Service points out, the defendant does not take any□
take into account certain processing methods such as the number of cameras, their location and□
does not substantiate some of these assertions. At no time does it examine the need for□
collection of these data, even though the text of the Protocol which constitutes the legal basis□
claimed states that "EASA and ECDC do not recommend taking the temperature of□
passengers to allow them to travel with 'immunity passports'. The agency recalls□
that the relevance of this test is not supported by current scientific knowledge about□
of SARS-CoV-2. 69 (see paragraph 99).□

248. In other words, the DPIA carried out by the defendant does not constitute a genuine□

analysis of processing operations and all their modalities from the point of view of the necessity and

proportionality. However, this review was particularly important given the lack of a framework

69 Protocol p. 5.

Decision on the merits 47/2022 - 48/73

provided by the claimed legal basis which granted significant leeway to the party

defendant in the choice of processing operations.

249. Based on the above considerations, the Litigation Chamber finds a violation of Article

35.7.b) GDPR.

On the assessment of the risks to the rights and freedoms of data subjects (Article 35.7.c of the

GDPR)

Findings of the Inspection Service

250. BSCA S.A. analyzed the risks with regard to the confidentiality, availability and integrity of data,

but not the risks associated with “false positives” and “false negatives” given the impact that such

risk may have on the persons concerned

251. The IS also considers that the risk of data availability and integrity has not been

sufficiently taken into account and that the RT could not correctly assess the risk of availability

that could arise in the event of unavailability of data.

252. In addition, BSCA S.A. was unable to correctly assess the risk that could arise in the event

unavailability of data.

253. BSCA S.A. has also not assessed the integrity risk that could arise in a situation where the

parameters of the device used were to be modified (calibration on a lower temperature

at 38°C).

254. The risk analysis carried out by the concluding party is not, according to the inspection report, sufficient

since the DPIA is content to analyze the risks in relation to confidentiality, the availability

and data integrity.

Position of the defendant

255. For the defendant, the DPIA limits its analysis to just a few points, on the grounds that the tool proposed by the CNIL does not provide for the analysis of the other questions mentioned in the report inspection. The concluding party believes that it has chosen an official methodology, validated and provided by a Data protection authority recognized at European level. She legitimately couldn't knowing that the tool in question was going to be considered incomplete by the inspection service of ODA.

Decision on the merits 47/2022 - 49/73

256. The defendant adds that the risks of false positives or false negatives are not to be analyzed in the framework of this procedure because it does not see how these risks are within its remit or should impact the processing of body temperature data. The defendant declares that it does not have carried out PCR tests, and that the notions of false positives or negatives therefore did not exist in the treatment she was doing.

257. The defendant recalls that after the third body temperature test (the anamnesis), she did not never prevented someone from accessing the terminal. The persons concerned have themselves decided not to enter the terminal.

258. Concerning the inaccuracies or lack of completeness mentioned by the inspection service as to the risks of availability and integrity, the defendant notes that the inspection service considers that its analysis is not sufficiently substantiated and takes due note of the improvements to be made place in the framework of the next DPIA that it will have to carry out.

Examination by the Litigation Chamber

259. For the Litigation Division, it appears that the risk analysis carried out by the party defendant is deficient. For example, to the question “2.1 What could be the main impacts on data subjects if the risk [of illegitimate access to data] occurs? », the defendant responds “limited impact”. This extremely brief answer demonstrates in any way that the defendant has thought about the risks of illegitimate access to Datas. In other words, the defendant does not indicate the risks that could

weigh on an affected person if a photo of themselves showing a higher temperature□

at 38°C had just been obtained by a third party.□

260. Similarly, during the assessment of risk 4: “disappearance of data”, the information given by□

the defendant are equally sketchy. The defendant states on several occasions that□

the risk is “not applicable (no storage)”, which is incorrect information□

since there is indeed a recording of the images, even if it is limited in time.□

The Litigation Chamber also considers here that the defendant has not demonstrated that it□

has carried out a correct and complete risk analysis.□

261. The Litigation Chamber also considers that the defendant failed to examine□

certain risks in its DPIA. The defendant indicates that the risks examined are those□

which are contained in the tool made available by the CNIL. However, this cannot excuse the absence□

taking into account certain identified risks. Indeed, Article 35.7.c) also mentions□

expressly “an assessment of the risks to the rights and freedoms of data subjects”.□

We do not see how an additional document could confirm what the legal text□

already mentioned. In addition, in its Recommendation No. 01/2018, the APD indicates in particular that the□

Decision on the merits 47/2022 - 50/73□

following elements must be considered as risks: financial losses, the situation□

where data subjects cannot exercise their rights and freedoms or are prevented□

to exercise control over their personal data; and any other economic damage□

or socially important⁷⁰.□

262. Recommendation No. 01/2018 indicates that “the loss of an opportunity” and the “denial or limitation□

access to places or events that are usually accessible to the public” are examples□

violations of rights and freedoms. For the Litigation Chamber, the fact of refusing access to the terminal□

to data subjects and preventing them from taking a flight may constitute an infringement□

rights identified or a risk as identified in the recommendation. As such, these risks□

should have been considered by the defendant. The Litigation Chamber considers that a□

example of such an analysis was carried out by the defendant in its pleadings□

responding to finding 5 of the Inspection Service regarding the violation of the principle of□

confidentiality and the obligation to put in place technical and organizational measures in□

with a view to securing data (see points 274 et seq.) and finding 6 on the principle of data protection□

data from design and by default (point 291 et seq.) . The Litigation Chamber regrets□

that this analysis was not included in the DPIA as it should have been.□

263. The Litigation Division also finds no impact analysis carried out at the time of□

the elaboration of the legal basis allegedly founding the processing. It was all the more important□

for the defendant to carry out a full risk analysis⁷¹.□

264. The Litigation Chamber therefore finds a violation of Article 35.7.c).□

On the measures envisaged to deal with the risks (article 35.7.d of the GDPR)□

Findings of the Inspection Service□

265. In view of the foregoing, the Inspection Service notes that, having failed to assess the□

risks to the rights and freedoms of the persons concerned, BSCA S.A. was unable to analyze the□

measures likely to deal with these risks in accordance with Article 35.7.d. of the GDPR.□

70 Data Protection Authority, Recommendation n° 01/2018 of February 28, 2018, §46. Available on□

<https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2018.pdf>.□

71 Article 35.10 of the GDPR indeed provides that a data controller may be exempted from carrying out an impact analysis if□

this has already been carried out during the development of the standard provided for in Article 6.1.c), which does not seem to b

Decision on the merits 47/2022 - 51/73□

Position of the defendant□

266. For the defendant, this assertion is not entirely correct. In fact, she says she has□

carried out an analysis of the measures based on the criteria included in the CNIL tool. It is so□

It is wrong to say that this assessment is impossible without further supporting it.□

267. For the defendant, it would have been desirable for the Inspection Service to check how and why□

the measures envisaged were not sufficient in view of the risks which emerged from the DPIA□

made by the defendant.□

268. Without foundation, it considers that it is not possible to consider that a breach is to be deplored□
on the part of the defendant.□

Examination by the Litigation Chamber□

269. Like the IS, the Chamber finds that breaches of Rule 35.7(a), (b) and (c) render□
impossible to correctly assess the measures to deal with the risks, which have not been□
assessed. For the Litigation Chamber, Article 35.7.d has therefore been violated.□

Concluding remarks□

Findings of the Inspection Service□

270. Furthermore, the Inspection Service wishes to emphasize that, given the findings made, it□
did not consider it appropriate to analyze each of the elements of BSCA S.A.'s DPIA insofar as the□
Inspection Service considered that these findings alone were sufficient to establish the□
violation of section 35.7. of the GDPR.□

Position of the defendant□

271. The defendant does not respond to the findings of the Inspection Service on this point.□

Examination by the Litigation Chamber□

272. In conclusion and in view of the elements specified above, the DPIA carried out by the defendant□
does not constitute a sufficiently detailed and complete exercise to fulfill the conditions of□
GDPR Article 35.7. Indeed, the document presented is more like a description and validation□

Decision on the merits 47/2022 - 52/73□

of the treatment that was already in place rather than a real risk assessment exercise for the□
rights and freedoms of the persons concerned and an overall reflection on the implementation of this□
system. On the basis of the above points, the Litigation Chamber therefore finds a violation of□
section 35.7.□

II.3.7 Finding 5: Violation of the principle of confidentiality and the obligation to□

put in place technical and organizational measures to secure the data□

(article 5.1.f and 32 of the GDPR)□

Findings of the Inspection Service□

273. The Inspection Service finds that BSCA S.A. has breached the principle of confidentiality and the obligation to□
put in place appropriate measures to guarantee the security of data in violation of the□
articles 5.1.f. and 32 GDPR. This observation is based on the fact that the identifiers and passwords□
passwords used to access the computer controlling the thermal cameras are included in the□
Memo communicated to X and to the defendant's firefighters, which entails a risk□
consultation of the data by a person other than those authorized.□

Position of the defendant□

274. For the defendant, a risk can be defined as “a scenario which describes an event and its□
effects, estimated in terms of severity and probability”.□

275. The analysis of the risk underlying unauthorized access to the computer connected to the cameras imposes the□
conclusion that the measures in place reduce this risk to an extremely low level (or even zero)□
both in terms of likelihood and severity and therefore the measures in place are□
adapted to the risk as required by Article 32 of the GDPR.□

276. The defendant considers that the PC in question is never accessible by anyone other than□
firefighters or X staff and even if a person had access to this room and□
to this computer, even if she had to have access to the codes available in the memo kept□
by firefighters. But this is highly unlikely according to her.□

277. With regard to the risk, the defendant argues that an unauthorized person would have had access□
to this computer by possessing the access codes, but she would not have had access to any data□
personal since the system erases the data during a reboot. Now, as the staff of X□
was present during all opening hours of the airport, with the fire brigade, no other□
no one would have had access to the room in which the data was processed during the day.□

Decision on the merits 47/2022 - 53/73□

Examination by the Litigation Chamber□

278. Article 5.1.f) of the GDPR establishes the principle of integrity and confidentiality. It is reproduced below

below:

“1. Personal data must be:

[...]

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

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

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

privacy); »

Recital 39 of the GDPR adds that “Personal data should be processed as

manner to ensure appropriate security and confidentiality, including to prevent unauthorized access

authorized to these data and to the equipment used for their treatment as well as the unauthorized use

of this data and this equipment”

279. This principle is further detailed in Article 32 which concerns the security of processing and which

is worded as follows:

“Rule 32

Processing security

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

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

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

subcontractor implement the appropriate technical and organizational measures in order to

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

has)

b)

pseudonymization and encryption of personal data;

means to guarantee the confidentiality, integrity, availability and

ongoing resilience of processing systems and services;

vs)□

means to restore the availability of personal data and□

access to them within appropriate timeframes in the event of a physical or technical incident;□

Decision on the merits 47/2022 - 54/73□

d)□

a procedure to regularly test, analyze and evaluate the effectiveness of□

technical and organizational measures to ensure the security of the processing.□

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

presents the processing, resulting in particular from the destruction, loss, alteration,□

unauthorized disclosure of personal data transmitted, stored or otherwise processed□

otherwise, or unauthorized access to such data, accidentally or unlawfully.□

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

certification approved as provided for in article 42 can be used as an element to demonstrate compliance□

of the requirements provided for in paragraph 1 of this article.□

4. The controller and the processor shall take measures to ensure that any□

natural person acting under the authority of the controller or the processor,□

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

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

280. According to the IS, the data concerned is at risk of consultation by an unauthorized person from the□

fact that the password and login to access the computer connected to the thermal cameras are all□

two available on the Memo communicated to X of Belgium.□

281. On the basis of the elements provided by the defendant, the Litigation Chamber considers that this□

risk is unlikely. Unauthorized access could only take place if all□

following circumstances were encountered:□

- Have access to X's memo;□

- Have access to the premises with the PC. According to the defendant, the PC is still occupied by□

a team during the opening hours of the airport for departures, and during arrivals from passengers coming from red zone at arrivals. . It therefore seems impossible for a person third party to use the computer given the presence of the teams.

- Can connect with logins and password.

The Litigation Chamber therefore considers that the probability of the risk of unauthorized access is very weak.

282. Furthermore, the Litigation Division agrees with the defendant's conclusion, which indicates that even in the event of unauthorized access to the PC, the third party would at best only have access to the 20 latest photos of people with a temperature above 38°C. This personal data, apart from the specific context of its processing and a possible refusal of entry into the terminal,

Decision on the merits 47/2022 - 55/73

is a fact that in itself involves little risk and is not very intimate, the vast majority of people who have had a fever at some point in their life. Furthermore, if a non-authorized access took place after the PC was shut down at the end of the day, all images would then already have been erased. The Litigation Chamber therefore considers that the security risk is very low, and that a violation of article 5.1.f and 32 of the GDPR cannot be accepted.

283. However, it generally recommends, as a security measure, to avoid keep the login and password on the same document. Thus, if the password can be kept on the memo, it is clearly more secure to send it by a communication mode different (email, SMS, etc.) which also makes it possible to ensure more frequent renewal and password easy.

284. For the Litigation Chamber, the Respondent should have demonstrated its correct assessment security risks when carrying out the DPIA. She can only regret that the three pages arguments and explanations found in the conclusions of the defendant did not incorporated into the corresponding part of the DPIA. It refers in this respect to these conclusions below above (see point 262).

II.3.8. Finding 6: Violation of the principle of data protection by design

and by default (article 25 of the GDPR)

Findings of the Inspection Service

285. For the Inspection Service, given the potentially serious risks to the rights and

freedoms of data subjects implied by the use of smart cameras whose

thermal cameras are part of it, it is essential that the data controller takes

appropriate measures to guarantee the effectiveness of the principles of data protection from the

design and default. This is all the more important if the processing in question involves

sensitive data, namely data concerning health.

286. First of all, the Inspection Service considers that by not carrying out the DPIA before the establishment of the

processing, the defendant was unable to properly document and analyze the various

appropriate measures. It refers in that regard to those findings above (see paragraph 262).

287. The Inspection Service notes that the thermal cameras retain the last twenty images

alert in the cache memory (RAM) of the thermal camera management software that is

erased gradually as well as when the computer is shut down (which takes place every evening). For the

Inspection Service, this temporary storage is not necessary to isolate people

and carry out further checks (on arrival) or to inform them of the symptoms

Decision on the merits 47/2022 - 56/73

potentials of COVID-19 (initially). A simple visualization of alerts in real time would be

sufficient.

288. Furthermore, the Inspection Service considers that the defendant did not inquire about the

storage with the camera supplier, when it should have been and the supplier himself

even questioned the defendant about it.

289. Finally, the Inspection Service considers that checking the temperature of those accompanying

is not necessary to achieve the purpose described. He adds that the title of the Protocol referring

to temperature control only applies to passengers and not accompanying persons.

290. On the basis of these elements, the Inspection Service finds that BSCA S.A. violated both the principle of minimization of data as well as the principle of data protection by the design of the articles 5.1.c. and 25 GDPR.

Position of the defendant

291. The defendant considers first of all that the findings of the Inspection Service show a lack of practicality. It considers that the analysis of the Inspection Service lacks an in-depth analysis of the situation. In fact, given the number of people passing through the terminal each day, it is not possible to arrest all people with a temperature above 38°C immediately at the precheck level. It is therefore necessary to record the images of the cameras so that people can be recognized and identified. Without these records, there is a risk of missing identified people. The defendant does not see how it could have operate the system with a “simple visualization of alert images in real time”, as suggested by the Inspection Service.

292. The defendant adds that the recorded images are limited to a maximum of 20 at a time and that they are systematically erased at the end of a day, i.e. after a maximum of 5 p.m. (4 a.m. to 9 p.m.).

293. It refutes the finding that it did not question the subcontractor about the deadline for conservation, indicating that this conclusion cannot be drawn from the very brief exchange of emails quoted.

294. The defendant also fails to see how it could have avoided processing the data of the accompanying persons as soon as they arrive at the airport, except to sort between the accompanying persons and travellers, which does not seem reasonable to him either in human terms or in terms of organizational. It indicates that it has also communicated on its website that access to the terminal is reserved for travelers in possession of a valid plane ticket, but it was difficult for them to refuse an accompanying adult to accompany their child in the terminal. She adds that

Decision on the merits 47/2022 - 57/73

these also constitute a health risk from the moment they enter the airport.

The concluding party considered, for the purposes of the application of the Mandatory Protocol which was imposed and given its organization, that anyone passing through the precheck was a passenger within the meaning of the Protocol.

Examination by the Litigation Chamber

295. The findings of the Inspection Service are based on Articles 5.1.c) and 25 of the GDPR, which relate respectively to the principle of data minimization and the principle of data protection.

data by design and by default. They are reproduced below:

“Clause 5

Principles relating to the processing of personal data

1. Personal data must be:

[...]

a) adequate, relevant and limited to what is necessary in relation to the purposes for

which they are processed (data minimization); »

“Rule 25

Data protection by design and data protection by default

1. Considering the state of knowledge, the costs of implementation and the nature, scope, the context and purposes of the processing as well as the risks, including the degree of probability and severity varies, whether the processing presents for the rights and freedoms of natural persons, the controller implements, both at the time of determining the means of the processing only at the time of the processing itself, the technical and organizational measures appropriate, such as pseudonymization, which are intended to implement the principles relating to data protection, for example data minimization, in an effective and to provide the processing with the guarantees necessary to meet the requirements of this Regulation and to protect the rights of the data subject.

Decision on the merits 47/2022 - 58/73

2. The controller implements the technical and organizational measures

appropriate to ensure that, by default, only personal data that is necessary with regard to each specific purpose of the processing are processed. This applies to the amount of personal data collected, the scope of their processing, their duration of preservation and accessibility. In particular, these measures ensure that, by default, personal data are not made accessible to an indefinite number of natural persons without the intervention of the natural person concerned.

3. A certification mechanism approved under Article 42 may serve as an element for demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this article. »

296. The principle of minimization is a key principle in the implementation of the principle of protection of data from design and by default, being directly referenced in the first and second paragraph of article 25.

297. These articles impose various obligations on the data controller which may be summarized as follows. First of all, only the data necessary to carry out the purpose must be processed (article 5.1.c of the GDPR). Then, the data controller must put in place appropriate technical and organizational measures intended to implement implements the principles relating to data protection (Article 25.1 of the GDPR) . Finally, the manager processing must put in place appropriate technical and organizational measures to ensure that, by default, only personal data that is necessary in relation to each specific purpose of the processing are processed (Article 25.2 of the GDPR).

298. Firstly, the Litigation Division concurs with the Inspection Service on the fact that compliance with these obligations should have been demonstrated in the DPIA that the data controller had to performed before starting treatment. The Litigation Chamber refers in this respect to these findings above (see paragraph 262). However, it will base its analysis on the elements additional information provided by the defendant in its pleadings.

299. It appears from the documents in the file that the data being processed was the temperature and a photo taken by cameras of people with a temperature above 38°C who

wish to enter the terminal or who are passengers returning from the red zone. She notices

also that a maximum of 20 photos were kept simultaneously and that these were

gradually replaced by older photos according to the “first in, first out” principle.

According to the defendant, these photos were deleted at the end of the day, which implies that

the photos were kept for a theoretical maximum duration of 17 hours. This treatment should

identify people wishing to enter the terminal or arriving from a zone flight

red and having a temperature above 38°C.

Decision on the merits 47/2022 - 59/73

300. In its investigation report, the Inspection Service considers that this retention period is too

long and that it is not necessary to isolate people and carry out checks

(initially) or to inform them of potential symptoms of COVID-19 (at

the arrival). A simple visualization of alerts in real time would be sufficient.

301. The Litigation Chamber finds that the data controller limited himself to the collection of two

types of data: temperature, as well as a photo to identify the person with a

temperature above 38°C. The photos are kept for a maximum of 17 hours. The

temperature is the data collected and the photo the data allowing the identification of the person

having a temperature above 38°C. The Litigation Chamber judges that in this situation,

the temporary preservation of the photo is necessary to allow the correct identification of the

concerned person. Indeed, limiting oneself to a single visualization in real time would require that the

person concerned can be arrested immediately, which could prove to be very complex

in the event of an influx of passengers. In addition, the temporary preservation of a photo can be

necessary to ensure that the person arrested is indeed the person concerned by the

treatment. As such, the duration and methods of storing images are necessary to

achieve the purpose of the processing, since a more restrictive method could lead to

disproportionate practical difficulties in pursuing the purpose.

For the Litigation Chamber, the defendant has indeed implemented technical measures

and organizational in order to limit the risks of processing. □

302. The Litigation Chamber also notes that particular attention seems to have been paid to □

minimization of data, since no registration of the identity of the persons concerned □

takes place and that the only anonymous register of the number of persons concerned was destroyed □

weekly. □

303. With regard to the processing of data of accompanying persons, who are therefore not □

passengers, the Litigation Chamber refers to its conclusions under finding 2 regarding the □

purpose of the processing. It recalls that the purpose declared by the defendant consists in "ensuring the □

health security of people transiting through the airport and employees working in the □

terminal" (see points 191 et seq.). The purpose of the processing is therefore not limited to taking □

temperature of passengers, but of all people wishing to enter the terminal. □

As such, the taking of the temperature of the accompanying persons is in accordance with the purpose. □

304. The Chamber finds that there was no violation of the data minimization principle (Article □

5.1.c of the GDPR) and the principle of data protection by design and by default (article 25 □

GDPR). □

Decision on the merits 47/2022 - 60/73 □

II.3.9 Finding 7: Violation of the obligation to keep a register of processing activities □

complete (article 30.1 GDPR) □

Findings of the Inspection Service □

305. The Inspection Service finds that the register does not contain all the mandatory information □

to be mentioned in a register of processing activities in accordance with Article 30.1. □

of the GDPR, the information below being missing: □

- □

- □

- □

The name and contact details of the data controller, namely BSCA S.A. The document □

includes a column "controller" which mentions the person(s) ☐

natural person(s) in charge of the processing within BSCA S.A.; ☐

The name and contact details of the data protection officer; ☐

The categories of recipients to whom the personal data have been or will be ☐

communicated. ☐

Position of the defendant ☐

306. The defendant admits the breach concerning the name and contact details of the person responsible for ☐

processing, and of the Data Protection Officer and provided an updated version of its ☐

register. ☐

307. With regard to the categories of recipients, the defendant considers that the Service ☐

inspection adds categories that are not provided for by the GDPR, since the latter does not impose ☐

not to specify the entity concerned or the category of subcontractor concerned. ☐

Examination by the Litigation Chamber ☐

308. The Inspection Service criticizes the defendant for not having complied with Article 30.1 of the ☐

GDPR. This article is reproduced below: ☐

"Rule 30 ☐

Register of processing activities ☐

1. Each controller and, where applicable, the controller's representative ☐

keep a record of the processing activities carried out under their responsibility. This register ☐

includes all of the following information: ☐

has) ☐

the name and contact details of the controller and, where applicable, of the joint controller ☐

processing, the representative of the controller and the data protection officer ☐

data; ☐

Decision on the merits 47/2022 - 61/73 ☐

the purposes of the processing; ☐

b)□

c) a description of the categories of data subjects and the categories of personal data□

personal;□

d)□

e)□

the categories of recipients to whom the personal data have been or will be□

communicated, including□

recipients in third countries or organizations□

international;□

where applicable, transfers of personal data to a third country or to a□

international organisation, including the identification of this third country or this organization□

international community and, in the case of transfers referred to in the second subparagraph of Article 49(1), the□

documents attesting to the existence of appropriate guarantees;□

f) as far as possible, the deadlines provided for the erasure of the different categories of□

data;□

g) as far as possible, a general description of the technical security measures and□

organizational arrangements referred to in Article 32(1).□

309. The Litigation Chamber finds that the defendant admits the breach concerning the name□

and the contact details of the data controller and the data protection officer (article□

30.1.a) and provided an updated version of its register. The name and contact details of the manager□

of processing as well as the data protection officer appear.□

310. With regard to the categories of recipients to whom the personal data have□

been or will be communicated, the Chamber notes that Article 30.1d of the GDPR requires the mention□

“categories of recipients to whom the personal data have been or will be□

communicated”. The term recipient is defined in article 4.9 of the GDPR as being “the person□

natural or legal person, the public authority, the service or any other body which receives communication□

personal data, whether or not it is a third party".

311. The question presented for consideration by the Litigation Chamber is that of the degree of precision with which the categories of recipients must be identified in the Register of the activities of treatment.

312. The register of the defendant's processing activities contains a heading entitled "Recipient? ".

This title contains several tabs structured as follows:

-

-

-

-

-

a "subcontractor" tab containing two options "yes" and "no";

an "application used" tab, under which the name of the application is entered;

an "internal or external application" tab, allowing you to select one of these two options;

a "digital/paper" tab allowing you to select one of these two options;

a "Country 1/3 (outside the EU)" tab under which the answer "no" systematically appears.

Decision on the merits 47/2022 - 62/73

313. Recommendation No. 06/2017 of 14 June 2017 of the CPP, relating to the Register of activities of processing (Article 30 of the GDPR) addresses this issue⁷². It specifies that are therefore covered, both potential internal and external recipients (such as subcontractors or third parties), established in the European Union or outside it. By way of example, the explanatory note of the declaration prior to processing mentions: the personal relationships of the data subject, the employers, other departments or companies of the data controller, social security, police and justice, brokers of personal data or direct marketing etc.

(Annex 1). »

314.□

It therefore appears from the text of the GDPR, supported by a recommendation from the CPP and doctrine⁷³□
that if it is not necessary to indicate the individual recipients of the data, it is on the other hand□
necessary to group them by category of recipients. The simple fact of only indicating whether it□
whether it is a subcontractor or not therefore does not meet this requirement.□

315. Based on the above elements, the Litigation Chamber finds a violation of Articles 30.1a□
and 30.1.d GDPR.□

II.3.10 Finding 8: Violation of the obligation to guarantee the independence of the Chief□
data protection in accordance with article 38.3. GDPR□

Findings of the Inspection Service□

316. The Inspection Department notes that BSCA S.A. did not ensure that the DPO did not receive any□
instruction with regard to the exercise of its missions in violation of Article 38.3. GDPR,□
in particular because of its position in the organization chart of the company, and its obligation□
to report to the General Counsel.□

Position of the defendant□

317. The defendant considers that the conclusions of the Inspection Service are not correct. She□
considers, citing the supporting guidelines, that the Inspection Service has not carried out an analysis□
of the independence of the DPD, but was content to take information from the organizational chart and□
does not demonstrate how he receives instructions concerning the performance of his duties. This one□
should have been made on concrete shortcomings. For the defendant, the fact of participating in□
“inter-departmental” meetings does not constitute a demonstration of its lack of independence, but□

72 Available at: <https://www.autoriteprotectiondonnees.be/publications/recommandation-n-06-2017.pdf>□

73 W. Kotschy, “Article 30: records of processing activities”, in Ch. Kuner The EU General Data Protection Regulation (GDPR),
commentary, 2020, p. 621.□

Decision on the merits 47/2022 - 63/73□

good for his involvement in the company. The defendant refers to the answer it already had□

sends to the Inspection Service and which establishes that the DPO is part of the legal service,□

reports annually to Management and receives an annual budget.□

318. During the hearing, the respondent's DPO made it known that his position in the company is□

clear and that he had a listening direction. He added that he previously reported to the legal director□

and worked in the legal department. Today the legal director has become the number 2 of□

the company and the DPO is therefore directly under his authority, even if he remains on the payroll of the□

Legal Department.□

Examination by the Litigation Chamber□

319. The Inspection Service finds a violation of Article 38.3 of the GDPR. This is reproduced below□

below:□

“Rule 38□

Function of the data protection officer□

1. The controller and the processor shall ensure that the data protection officer□

data is involved, in an appropriate and timely manner, in all questions relating to□

the protection of personal data.□

2. The controller and the processor assist the data protection officer in□

carry out the tasks referred to in Article 39 by providing the resources necessary to carry out□

these tasks, as well as access to personal data and processing operations,□

and allowing him to maintain his specialized knowledge.□

3. The controller and the processor shall ensure that the data protection officer□

data does not receive any instructions with regard to the performance of the tasks. The delegate to the□

data protection cannot be relieved of his duties or penalized by the person responsible for the□

processing or the subcontractor for the exercise of its missions. The delegate for the protection of□

data reports directly to the highest level of management of the head of the□

processor or processor. »□

320. According to the IS, the data controller failed to fulfill the obligations provided for in Article 38.3,□

since the positioning of the DPO under the direction of the legal director of the defendant□

Decision on the merits 47/2022 - 64/73□

and the fact that he must report to her every two weeks contravenes the prohibition on receiving□

“instruction[s] regarding the exercise of the missions. ”.□

321. The Article 29 Working Party has drafted guidelines on the DPO which have been taken up by□

the EDPS⁷⁴. On the question of the independence of the DPO, the guidelines contain the□

following paragraphs:□

“This means that, in the exercise of their tasks under Article 39, DPOs must not□

receive instructions on how to handle a case, for example, what outcome should be□

obtained, how to investigate a complaint or whether to consult the supervisory authority. In addition,□

they cannot be required to adopt a certain point of view on a question relating to the legislation in question.□

data protection, for example, a particular interpretation of the law.□

[...]□

If the controller or processor makes decisions that are incompatible with□

the GDPR and the opinion of the DPO, the latter should have the possibility to clearly indicate his opinion□

diverge at the highest level of management and decision makers. »⁷⁵□

322. It therefore appears from the guidelines that the question of the independence of the DPO is based on two□

different criteria: first, its independence must be assessed in a contextual and independent manner.□

situ, i.e. it must be ensured that the DPO has not been subjected to any influence or pressure□

on how he must exercise the duties imposed on him under the GDPR. It would therefore be□

here of an obligation to refrain from interference with its missions and the absence of imposition of□

retaliatory measures. A second obligation that comes from the text of the GDPR and the guidelines□

is a positive obligation this time, and which requires the data controller to guarantee that the□

DPD can account for its opinions and its work at the highest level of the hierarchy. It's about□

here of an additional form of protection which should allow the DPO to make his voice heard within□

organisation.□

323. The Litigation Chamber finds in this case that the second obligation, which is to be able to

reporting to the highest level of the hierarchy is not called into question by the IS.

324. On the other hand, the Inspection Service considers that the position in the organization chart of the DPO is detrimental

to his independence since he contravenes the first obligation, which is that of not undergoing

interference in his work. The Litigation Chamber, as explained above, considers

however, it cannot be deduced from a position in the organizational chart and from an obligation to

74 Article 29 Data Protection Working Party, Guidelines for Data Protection Officers

(DPD), adopted on 13 December 2016. Available at: <https://ec.europa.eu/newsroom/article29/items/612048>.

75 Ibid, p. 18. It is the Litigation Chamber which highlights.

Decision on the merits 47/2022 - 65/73

report to the General Counsel every two weeks that the DPO receives instructions that

jeopardize his independence. This evaluation must be made on the basis of concrete indices

interference which is not brought here. The GDPR does not prohibit the DPO from having a superior

hierarchical.

325. Article 38.3 of the GDPR also specifies that “the data protection officer cannot be

relieved of his duties or penalized by the controller or processor for

the performance of its duties”. However, it appears from the documents in the file and in particular from the response that the

defendant brought to the questions of the Litigation Chamber in preparation for

the hearing, that the DPD was very frequently on technical unemployment between May and August 2020. The

defendant provides the following statement in this regard:

“In fine, here is the total count of the days worked by the DPO of the defendant between April 2020

and August 2020:

- Three (3) days during the month of April 2020;

- Five (5) days during the month of May 2020;

- Three (3) days during the month of June 2020;

- Nine (9) days during the month of July 2020; and finally

- Thirteen (13) days during the month of August 2020.”⁷⁶

326. It appears from these documents that, between April 2020 and August 2020, the DPO only worked 33 days at total. ⁷⁷

327. The Respondent's response indicates that a large part of its staff was in technical unemployment at that time. The Litigation Chamber cannot therefore conclude that the DPD has been particularly targeted by this economic unemployment and “penalized for the exercise of his assignments” within the meaning of Article 38.3.

328. However, it is clear from the figures given above that during preparation for the commissioning processing (in June 2020-, the DPO only had very few working days workforce. The Litigation Chamber therefore doubts that he could have been "associated, in a way appropriately and in a timely manner, to all questions relating to the protection of personal data personnel” as required by Article 38.1 of the GDPR. The Litigation Chamber has duly taken note the fact that a note was requested from the DPO on April 30, 2020 on the legality of the processing of catches temperature and that the latter responded the same day to this request with a brief note of 2.5 pages. She also noted that the file contained certain email exchanges involving the DPO

⁷⁶ Letter of October 18, 2021, p. 5.

⁷⁷ Ibid.

Decision on the merits 47/2022 - 66/73

during the period concerned. However, it considers that this does not in itself constitute proof adequate and timely association of the DPO.

329. On the contrary, the Litigation Chamber questions the fact that the DPO was laid off technical during the period of implementation of the disputed processing, which could have impairment of his ability to be “associated, in an appropriate and timely manner”⁷⁸ with the reflection regarding such processing. The Litigation Chamber considers that the decision to put the DPD on technical unemployment is likely to prevent it from performing its duties in accordance with

GDPR Article 38.1. However, the Trial Chamber does not have sufficient information to
rule in this regard in the particular case and find a violation.

III. Violations and Penalties

330. Under Article 100 LCA, the Litigation Chamber has the power to:

1° dismiss the complaint without follow-up;

2° order the dismissal;

3° order a suspension of the pronouncement;

4° to propose a transaction;

5° issue warnings or reprimands;

6° order to comply with the data subject's requests to exercise
his rights;

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

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

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° impose periodic penalty payments;

13° to impose administrative fines;

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

15° forward the file to the public prosecutor's office in Brussels, which
informs him of the follow-up given to the file;

78 Article 38.1 of the GDPR.

Decision on the merits 47/2022 - 67/73

16° decide, on a case-by-case basis, to publish its decisions on the Authority's website□

data protection.□

331. As to the administrative fine that may be imposed under Articles 58.2.i) and 83 of the GDPR□

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

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

under this article for breaches of this Regulation referred to in paragraphs 4,□

5 and 6 are, in each case, effective, proportionate and dissuasive.□

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) of Article 58(2), and□

j). To decide whether to impose an administrative fine and to decide the amount□

of the administrative fine, due account shall be taken, in each case, of the□

following elements:□

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

or of□

the purpose of the processing concerned, as well as the number of persons□

concerned 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□

the subcontractor for□

mitigate the damage suffered by the persons concerned;□

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

the technical and organizational measures they have implemented pursuant to Articles□

25 and 32;□

e)□

any relevant breach previously committed by□

the
responsible for
processor or processor;
(f) the degree of cooperation established with the supervisory authority with a view to remedying the
violation and to mitigate any adverse effects;
g)
the categories of personal data concerned by
the violation
;
h) how the supervisory authority became aware of the breach, including
whether, and to what extent, the controller or processor has notified the
breach ;

Decision on the merits 47/2022 - 68/73

(i) where measures referred to in Article 58(2) have previously been
ordered against the controller or processor concerned
for the same purpose, compliance with these measures;
(j) the application of codes of conduct approved pursuant to Article 40 or
certification mechanisms approved under Article 42; and
k) any other aggravating or mitigating circumstance applicable to the circumstances of
the species,
such as
benefits
obtained or
losses avoided,
directly or indirectly, by reason of the breach.”

332. The Litigation Chamber recalls that the purpose of the fine is not to put an end to an offense

committed but to effectively enforce the rules of the GDPR. As it appears clearly from recital 148, the GDPR indeed provides that sanctions, including fines administrative, be imposed for any serious violation - therefore including at the first finding of a violation -, in addition to or instead of the appropriate measures which are imposed.⁷⁹ This same recital provides for two cases in which it is possible to waive a fine, i.e. for minor violations or where the fine would constitute a charge disproportionate to a natural person within the meaning of recital 148 of the GDPR, two cases which would waive a fine. The fact that this is a first finding of a violation of the GDPR committed by a data controller does not affect the possibility for the Litigation Chamber to impose an administrative fine. The instrument of the fine administrative action is in no way intended to put an end to the violations. To this end, the GDPR and the LCA provide for several corrective measures, including the orders cited in Article 100, § 1, 8° and 9° of the LCA.

333. In the present case, the Litigation Division found that the defendant had violated the following items:

a) Violation of Articles 6.1.c), 6.3, and 9.2.i), since it is not demonstrated that the processing of the personal data in question is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or for the purpose of ensuring standards high standards of quality and safety of health care and medicines or devices medical conditions, on the basis of Union law or the law of the Member State which provides for

⁷⁹ Recital 148 provides the following: "In order to strengthen the application of the rules of this Regulation, sanctions including administrative fines should be imposed for any violation of this Regulation, in addition to or instead of the appropriate measures imposed by the supervisory authority under this Regulation. In the event of a minor violation or if the fine liable to be imposed constitutes a disproportionate burden for a natural person, a warning may be issued rather than a fine. However, due consideration should be given to the nature, gravity and duration of the breach, the character

intent of the breach and the measures taken to mitigate the damage suffered, the degree of responsibility or any breach
relevant previously committed, the manner in which the supervisory authority became aware of the breach, compliance with
measures ordered against the controller or processor, the application of a code of conduct, and any
other aggravating or mitigating circumstance. The application of sanctions, including administrative fines, should be subject to
appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to
effective judicial protection and due process. [underlining by the Litigation Chamber]

Decision on the merits 47/2022 - 69/73

appropriate and specific measures to safeguard human rights and freedoms
concerned, in particular professional secrecy. In addition, the legal bases invoked by the
defendant (namely the Decree of 23 June 1994 relating to the creation and operation
airports and aerodromes within the Walloon Region, the ministerial decree of 30 June
2020 on urgent measures to limit the spread of the Covid-19 coronavirus,
the law of 31 December 1963 on civil protection (as replaced by the law of 15 May
2007) and the "Commercial Aviation Passengers" Protocol of June 11, 2020) do not meet
the requirements of Article 6.1 c) read in conjunction with Article 6.3 of the GDPR.

b) Violation of Articles 5.1.a), 12.1, 13.1c), 13.2.a), 13.2.d), and 13.2.e), for failing to
transparency vis-à-vis the persons concerned by not informing them that the taking of
temperature would be done using thermal cameras; for not having informed
correctly passengers returning from the red zone for not having correctly
informed of the legal basis of the processing, the purpose of the processing and the regulatory framework
the obligation to monitor body temperature; for not having correctly
informed of the data retention period and the right to lodge a complaint
with the Data Protection Authority.

c) Violation of

Article 5.1.b), given that

the purpose of the processing was not

sufficiently explicit□

when□

the treatment began, since she was not□

expressly stated in any source of information used by the defendant. The□

purpose of the processing was only explained in response to questions from the Inspection Service□

and after the modification of the privacy policy in December 2020.□

d) Violation of Articles 35.1 and 35.7 for not having carried out the Impact Assessment of the□

data protection prior to processing. In addition, the impact analysis□

is incomplete since it does not contain an adequate description of the operations of□

processing envisaged and the purposes of the processing, it does not sufficiently analyze the□

necessity and proportionality of the processing and does not correctly assess the risks for□

the rights and freedoms of data subjects.□

e) Violation of articles 30.1.a) and 30.1.d) due to the absence, in the register of activities□

processing, mention of the name and contact details of the processing manager as well as□

than the data protection officer at the time of the investigation and for lack of□

sufficient precision as to the categories of data recipients.□

334. Pursuant to Article 101 of the LCA, it decides to impose a fine of EUR 100,000 on the defendant□

for violations of Articles 5.1.a, 5.1.b, 6.1.c), 6.3, and 9.2.i), 12.1, 13.1c), 13.2.a), 13.2.d), 13.2.e), 35.1 and□

35.7.□

Decision on the merits 47/2022 - 70/73□

335. In view of Article 83 of the GDPR, the Litigation Chamber justifies the imposition of an administrative sanction□

in a concrete way⁸⁰, by retaining the following criteria, taken from this article, which it deems relevant□

in the present case:□

-□

the nature, gravity and duration of the violation (art. 83.2.a) — The violations found are□

in particular a violation of the provisions of the GDPR relating to the principles of the protection of□

data (Article 5 of the GDPR) and the lawfulness of the processing (Article 6 of the GDPR). A breach of the aforementioned provisions is, in accordance with Article 83 (5) of the GDPR, liable to the highest monetary penalties.

The infringements noted also concern the violation of the provisions relating to information and transparency obligations (articles 5.1.a), 12.1 and 13 of the GDPR). Respect for the above-mentioned provisions is essential and must take place at the latest at the start of the processing of personal data. This is also necessary to facilitate the exercise of rights of the persons concerned.

The infringements noted also concern the performance of the Impact Assessment relating to the

Data protection. This obligation was only fulfilled after the start of the treatment, so that it should have been carried out before (article 35.1 of the GDPR) and was not carried out in accordance with the criteria of article 35.7, which considerably affected the credibility of the exercise and the potential rights benefits.

- Any relevant breach previously committed by the controller or sub-

(art.83.2.e) GDPR)— The defendant has never been the subject of infringement proceedings before the Data Protection Authority.

-

the categories of personal data affected by the breach (art.83.2.g) GDPR)—

The breaches identified relate to a category of personal data within the meaning of Article 9 of the LCA (data relating to the health of the persons concerned).

-

any other aggravating or mitigating circumstance applicable to the circumstances of the case (art. 83.2 k) GDPR): the defendant did not derive any benefit from the processing operations or the offenses committed.

336. All the elements set out above justify an effective, proportionate and

dissuasive, as referred to in Article 83 of the GDPR, taking into account the assessment criteria that it

contains.□

337. A sanction form was sent on February 15, 2022 to which the defendant responded on March 9□

2022. These arguments can be summarized as follows:□

80 Brussels Court of Appeal (Market Court section), X. v APD, Judgment 2020/1471 of 19 February 2020□

Decision on the merits 47/2022 - 71/73□

has. It was subject to the obligation to implement the processing. She had no choice□

and could not count on the guidance of the APD.□

b. The fine must remain an exceptional means, in particular in view of the case of force majeure□

in which the airport found itself and considering the fact that the treatment was very limited□

over time and is no longer in place today.□

vs. The airport suffered extremely high losses due to COVID and had to be□

recapitalized to avoid bankruptcy. This recapitalization was conditional on the conclusion□

a social agreement which provides for reductions in remuneration for employees (agreement□

reported in the press).□

338. The Litigation Division considers that the argument developed in point a) below has been the subject of□

developments in the body of the decision (see points 58 et seq.). The Litigation Chamber reiterates□

that the Protocol does not constitute a valid legal basis within the meaning of the GDPR and the defendant has□

recognized the lack of clarity of the Protocol and the fact that a law would have been preferable⁸¹. She returns□

also to point 232 regarding the lack of guidance.□

339. The Litigation Division has also already responded to point b) above (see points 217 et seq.) in□

the body of the decision. Regarding the fact that the processing was limited in time and is no longer□

currently in place, the Litigation Chamber recalls that it extended over a period□

approximately 9 months (between June 2020 and March 2021) for all departing passengers and accompanying persons,□

thus for a period of just over a month for people arriving from the red zone (September-□

October 2020). It also recalls that if the defendant was unable to provide a total number of□

data subjects, it indicated that for the sole period between June 15, 2020 and October 31,□

2020, approximately 457,000 departing passengers were screened. The processing can therefore neither be considered to have been very limited in time, nor in the number of people involved.

340. With regard to point c), the Litigation Chamber recalls that it is indeed the turnover that is used as the criterion for determining the maximum amount of fines in the GDPR and not the income statement. This choice by the European legislator was made on purpose in order to prevent variations in the income statement do not limit the ability of the supervisory authorities to data to impose effective fines.

341. The Litigation Chamber also emphasizes that the other criteria set out in Article 83.2 of the GDPR are not relevant in this case and therefore do not lead to an administrative fine other than than that determined by the Litigation Division in the context of this decision.

81 The Litigation Chamber will also send a copy of this decision to the competent minister.
Decision on the merits 47/2022 - 72/73

342. In accordance with the foregoing, the Litigation Division finds that it can rely on the annual figures from Brussels South Charleroi Airport SA to determine the amount of the fine administrative procedure which it intends to impose on the defendant.

343. The Litigation Chamber refers to the conclusions of the defendant filed with the Litigation Chamber as well as the annual accounts filed with the National Bank of Belgium (BNB) on July 5, 2021, which report a turnover for the financial year 2020 of EUR 28,859,291.41.

344. The planned administrative fine of 100,000.00 euros corresponds in this case to 0.34% of the annual business of the defendant for the year 2020. The Litigation Chamber refers the submissions of the defendant filed with the Litigation Chamber as well as the annual accounts filed with the National Bank of Belgium (BNB) on July 5, 2021, which are statement of turnover for the 2020 financial year of EUR 28,859,291.41.

345. The planned administrative fine of 100,000 euros corresponds in this case to 0.34% of the defendant's annual business for the year 2020.

346. The Litigation Division indicates that the maximum amount of the administrative fine for a violation is determined by Articles 83.4 and 83.4 GDPR. The amount of the fine imposed in this Decision is significantly lower than the maximum amount foreseen (which could have reached a maximum of EUR 1,154,371.65), given that the Litigation Chamber took into account all the relevant criteria set out in Article 83.2 LCA. In addition, the Litigation Chamber assesses the concrete elements of each case individually in order to impose an appropriate sanction.

347. For violations of Articles 30.1.a) and 30.1.d), the Litigation Chamber decides, under Article 100, §1, 5° of the ACL, to impose a reprimand. Indeed, the violations found relate to relatively minor elements, the violation of which does not in itself justify the imposition of a fine.

IV. Publication of the decision

348. Seen

the importance of

transparency regarding

the decision-making process of

bedroom

Litigation, this decision is published on the website of the Authority for the protection of data in accordance with article 95, §1, 8° LCA by mentioning the identification data of the defendant and this because of the specificity of this decision - which leads to the fact that even in the event of omission of identification data, re-identification is unavoidable - as well as the general interest of this decision.

Decision on the merits 47/2022 - 73/73

FOR THESE REASONS,

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

- Pursuant to Article 101 of the ACL, impose a fine of EUR 100,000 on the defendant for violations of Articles 5.1.a, 5.1.b, 6.1.c), 6.3, and 9.2.i), 12.1, 13.1c), 13.2.a), 13.2.d), 13.2.e), 35.1 and 35.7;
- Pursuant to Article 100, §1, 5° of the LCA, to impose a reprimand for violations of the

Articles 30.1.a) and 30.1.d);□

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

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

data protection as defendant.□

(Sr.) Hielke Hijmans□

President of the Litigation Chamber□