Litigation Chamber

Decision on the merits 24/2021 of February 19, 2021

File number: DOS-2020-02716

Subject: Counting passers-by at specific locations on the dike and in areas

merchants on the Coast using smart cameras in the context of Covid-19

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

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

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

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

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

data protection, hereinafter the "GDPR");

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

"LCA";

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:

- Westtoer APB (Autonomous Provincial Company), headquartered in Koning

Albert I-laan 120 - 8200 SINT MICHIELS (BRUGES) and whose company number is

0267.388.418, hereinafter "the defendant".

1. Facts and procedure

1. On July 9, 2020, the Management Board of the Data Protection Authority decides, in

pursuant to Article 63, 1° of the LCA, to seize the Inspection Service of a file because it has noted

serious indications that the defendant's use of smart cameras

could lead to a violation of the fundamental principles of data protection to

personal character.

2. More specifically, it was found that since June 27, 2020, several coastal municipalities

used smart cameras to measure crowds at certain locations in

the dike and in shopping areas of these municipalities in the context of the epidemic of

Covid-19. The defendant had issued a public contract for this purpose on behalf of the municipalities

concerned, which was awarded to company X, which acted as

processor within the meaning of Article 4.8 of the GDPR.

3. On July 16, 2020, pursuant to Article 66, § 1, 3° of the LCA, the Inspection Service sent

a written request to the respondent for information and documentation

additional information on the aforementioned processing activity, and more specifically on:

1)

the register of processing activities kept by the defendant in accordance with Article

30 GDPR;

2)

the number of smart cameras placed and active in the context of the public market

“Passantentellingen op specifieke locaties op de dijk en in winkelzones aan de Kust”

(Editor's note: Counts of passers-by at specific locations on the seawall and in

shopping areas at the Coast) issued by the defendant;

3)

compliance with the principles of lawfulness, fairness and transparency (Article 5.1 a) of the

GDPR), purpose limitation (Article 5.1 b) of the GDPR) and minimization of

data (Article 5.1 c) of the GDPR);

4)

the legal basis for the processing of personal data through the

smart camera system within the meaning of Article 6.1 of the GDPR, read together

with Articles 5.2 and 24.1 of the GDPR;

5)

carrying out a data protection impact assessment (Article 35

of the GDPR) in the context of the aforementioned public contract; and

Decision on the merits 24/2021 - 3/44

6)

the designation and position of the data protection officer (Articles 37 and

38 GDPR).

4. On August 13, 2020, the Inspection Service sends a reminder letter by e-mail to the defendant

concerning the aforementioned written questionnaire.

5. By e-mail of August 18, 2020, the Respondent informs the Inspection Service that the e-mail

through which the answers as well as the requested documents were communicated to the Service

of Inspection obviously never reached him.

6. By e-mail of August 18, 2020, the Respondent again sends the Inspection Service its

answers to the latter's questions as well as the documents requested.

The inspection report

7. On August 25, 2020, the Inspection Service sends its inspection report to the Chairman of the

Litigation Chamber, in accordance with Article 91, § 2 of the LCA, following which the Chamber

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

In its report, in the context of serious indications, the Inspection Service formulates the

following findings:

1) Violation of Articles 5.1 a) (principles of lawfulness, fairness and transparency), b)

(principle of purpose limitation) and c) (principle of data minimization) of the

GDPR and Article 5.2 GDPR (liability); in this regard, the Inspection Service

first declares that the defendant does not sufficiently demonstrate that the

data subjects are informed in a fair and transparent manner about the

processing of their personal data via smart cameras and

that the defendant's reference to "the privacy statement appearing on the sites

Internet of Westtoer, of which dekust.be" is too vague and imprecise.

quoted passages from the file have been freely translated by the Translation Service of

the Data Protection Authority, in the absence of an official translation]

Secondly, the Inspection Service states that the defendant does not demonstrate

enough that the processing of personal data via the cameras

intelligence in question takes place for specified, explicit and legitimate purposes.

Thirdly, the Inspection Service declares that the defendant does not demonstrate

sufficiently that the personal data processed via the cameras

intelligent are adequate, relevant and limited to what is necessary in view of

of the purposes for which they are processed.

2) Violation of Article 6.1 of the GDPR: the Inspection Service finds that the defendant

bases the processing of personal data by means of cameras

smart on article 6.1 e) of the RGPD and that it refers in this respect to the contract of

management concluded with the province of West Flanders, in which it is specified that

the defendant's mission is to support tourism in West Flanders.

The Inspection Service considers, however, that the defendant does not demonstrate why

the fulfillment of this mission of public interest requires the processing of data at

personal character via smart cameras. In this regard, the Inspection Service
draws attention to the fact that the ability to demonstrate this necessity is a
requirement under Article 6.1 e) of the GDPR read in conjunction with Articles 5.2
and 24.1 GDPR.
3) Violation of articles 12.1, 12.6, 13.1 and 13.2 of the GDPR: the Inspection Service
finds that the information provided by the defendant via the declaration of
confidentiality published on the website www.westtoer.be/nl/dataverwerking
are not entirely correct or transparent.
4) Violation of articles 35.2 and 35.7 of the GDPR: the Inspection Service finds that
the data protection impact assessment carried out by the respondent does not
does not meet the requirements set out in the aforementioned articles and that the delegate
to data protection has not been sufficiently involved.
In addition, the Inspection Service makes several additional findings apart from
the framework of serious indications, namely concerning:
1) a violation of Article 4.11 of the GDPR read in conjunction with Article 6.1 a) of the
GDPR as well as Articles 7.1 and 7.3 of the GDPR: the Inspection Service finds
in particular that on the defendant's website, continued browsing
on this website by the data subject is considered a
consent to the use of cookies.
2) a violation of Article 30.1 of the GDPR: the Inspection Service finds that the
record of the defendant's processing activities does not meet the requirements of
the aforementioned article. More specifically, the Inspection Service finds that:
i)
the contact details of the data controller are incomplete, since
the e-mail address mentioned in the privacy statement of the
defendant is not included therein;

ii)

the description of the categories of data subjects is incomplete,

seen from the mention "others" in the column "categories of people

physical";

iii)

third countries to which personal data is transferred

transferred are not mentioned, only the processing

email addresses via Mailchimp, without mentioning the countries in question; and

iv)

the register does not mention visitors to the website or the use of

Cookies.

3) No violation of Articles 37.5 and 37.7 of the GDPR regarding the designation of the

data protection officer.

4) Violation of Articles 38.2 and 38.3 of the GDPR and no violation of Article 38.6 of the

GDPR: the Inspection Service finds that the Data Protection Officer

is not employed full-time and that the latter does not report directly to the

highest level of management of the defendant.

8. On September 3, 2020, the Litigation Division decides, pursuant to Article 95, § 1, 1° and

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

9. By letter dated September 3, 2020, the defendant is informed that the file can be

treaty on the merits and, under Article 99 of the LCA, he is also informed of the time limit for

present their conclusions.

Defendant's submissions in response

10. On October 1, 2020, the Respondent files its submissions in response and also requests

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

11. In its submissions in response, the Respondent states with respect to the first

finding of the Inspection Service (violation of the principles of lawfulness, fairness and

transparency (Art. 5.1 a) GDPR), purpose limitation (Art. 5.1 b) GDPR) and

data minimization (Art. 5.1 c) GDPR) that this finding is incorrect in law

as in fact, given that the Respondent sufficiently informed the persons concerned at

regarding the processing of their personal data, via the declaration of

confidentiality included on the applicant's websites - including www.dekust.be - on the one hand

and via extensive press coverage and the issuance of a press release

on the other hand. The Respondent attaches the supporting documents and concludes that, given this significant

Decision on the merits 24/2021 - 6/44

communication, it can be assumed that the vast majority of visitors to the coast were at

current use of smart cameras.

12. The Respondent adds that contrary to what was found by the Inspection Service, the

passers-by counting system does indeed have a determined, explicit and

legitimate, namely to control the number and concentration of visitors to the coast within the framework

of the fight against the Covid-19 pandemic.

13. With regard to compliance with the principle of data minimization, the Respondent asserts

in its conclusions in response having previously carried out an in-depth analysis with

the processor and its data protection officer to ensure that

the use of the smart cameras in question is adequate, relevant and limited to what

is necessary for the intended purpose. The Respondent clarifies that the following measures

have been taken in order to limit the processing of data as much as possible: i) anonymization

personal data, ii) the short retention period of the personal data

personnel, iii) the limitation of the number and placement of cameras, iv) the short deadline for

measurement and (v) limited access to personal data.

14. The Respondent further explains with regard to the need for the use of the system of

smart cameras than alternative monitoring systems - such as counts

manuals or counts using wi-fi signals - are not accurate enough for the purpose

intended and that only the system used makes it possible to obtain certain additional information

which are necessary for the achievement of this purpose. The Respondent specifically asserts

that the respect or not of the rules of social distancing, the direction of circulation of the passers-by

and the different types of passers-by cannot be detected by any alternative system and

that only the smart camera system allows real-time reporting, which is

crucial to be able to communicate and, if necessary, intervene in a timely manner.

15. With regard to the second finding of the Inspection Service (lawfulness of the processing -

Article 6.1 of the GDPR), the defendant alleges that the passers-by counting system was

indeed necessary to accomplish the mission of public interest within the meaning of Article 6.1 e) of the

GDPR, namely to fight against the Covid-19 pandemic and ensure the safety of visitors to

the side. The defendant refers in this respect to the management contract with the province of Flanders

western. He specifically states that the smart camera system was the only

means of accomplishing the aforementioned public interest task, given that i) only metering via

smart cameras can provide sufficiently accurate data on the number

of visitors, ii) only counting via smart cameras makes it possible to obtain

crucial additional information and iii) only this system allows for reporting in

real time.

16. With regard to the findings of the Inspection Service relating to transparency

(Articles 12 and 13 of the GDPR), the respondent acknowledges that the privacy statement may

be improved, but he says he does not agree with the charges.

17. With regard to the findings of the Inspection Service regarding the impact assessment

relating to data protection (Articles 35.2 and 35.7 of the GDPR), the defendant submits

that the opinion of the data protection officer has indeed been collected and that this opinion

includes the mandatory information of article 35.7 of the GDPR; the defendant joins

supporting documents.

18. With regard to the findings of the Inspection Service relating to consent to

cookies on the defendant's website (articles 4.1, 6.1 a) and 7.1 of the GDPR), the latter

acknowledges that the cookie policy can be improved but affirms that it is

explained in the privacy statement how cookies can be deleted,

specifying that this is possible via the browser settings.

19. With regard to the findings of the Inspection Service relating to the register of activities

of processing (Article 30.1 of the GDPR), the defendant submits that it cannot be said that

Westtoer's contact details are incomplete only due to the lack of

the e-mail address dataverwerking@westtoer.be..

20. With regard to the findings of the Inspection Service relating to the position of the delegate

to data protection (Articles 38.2 and 38.3 of the GDPR), the defendant claims that the fact

that the latter exercises his function according to a 4/5 regime does not imply that he does not have enough

time to perform his duties. The Respondent emphasizes in this regard that the Group of

work "Article 29" on data protection clarified that a data protection officer

data did not necessarily have to carry out its duties full time. The defendant denies

this accusation and affirms that the actions of the delegate in this file concerning the system

counting of passers-by, and in particular the opinion of the latter, confirm that the delegate for the

data protection does have enough time to fulfill its

tasks. Finally, the defendant confirms that for his daily communication, the delegate

has a line with a Westtoer employee, but that the latter has the right and

the obligation to share important points with the hierarchy of Westtoer.

21. By letter dated December 9, 2020, the Litigation Chamber addresses several questions

additional information to the defendant for the hearing.

22. On December 15, 2020, the Respondent transmitted its written answers to the questions

aforementioned of the Litigation Chamber.

Decision on the merits 24/2021 - 8/44

The hearing

23. On December 16, 2020, the defendant was heard by the Litigation Chamber, in accordance

in article 53 of the rules of procedure.

24. During this hearing, the defendant demonstrates to the Litigation Chamber

view of the operation of the smart camera system used as a security system

counting passers-by.

25. On January 5, 2021, the minutes of the hearing are transmitted to the defendant, in accordance with

Article 54 of the internal rules.

26. On January 8, 2021, the Respondent informed the Litigation Chamber that he had no comments

concerning the aforementioned minutes of the hearing.

2. Motivation

2.1.

"Processing of personal data" and the jurisdiction of the Litigation Chamber

27. Article 4.1 of the GDPR defines the concept of "personal data" as being "any

information relating to an identified or identifiable natural person (hereinafter

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

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

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

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

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

28. In accordance with Article 4.2 of the GDPR, it is to be considered as "processing" of

personal data: "any operation or set of operations carried out

or not using automated processes and applied to data or sets of

personal data, such as the collection, recording, organization,

structuring, storage, adaptation or modification, extraction, consultation,

the use, communication by transmission, dissemination or any other form of

provision, reconciliation or interconnection, limitation, erasure or

destruction".

Decision on the merits 24/2021 - 9/44

29. The Court of Justice has confirmed on several occasions in its case-law that the taking of images

of people by cameras came under the concept of "personal data" in the

meaning of the standards of European data protection law. In his

Ryneš judgment, the Court of Justice clarified in this regard:

“It should be recalled that [...] this Directive [...]1 applies "to the processing of personal data

personal nature, automated in whole or in part, as well as non-automated processing

of personal data contained or required to appear in a file".

The notion of "personal data" [...] encompasses [...] "any information concerning

an identified or identifiable natural person". An identifiable person is "a person who

may be identified, directly or indirectly, in particular by reference to one or [...]

several specific elements, specific to his physical identity".

An image of a person taken by a camera therefore comes under the notion of data to be

personal nature within the meaning of the provision referred to in the previous point, since it allows

to identify the person in question.”.2

30. In the present case, it appears from the documents in the file and from the explanations provided by the

defendant at the hearing that the activity in question relates to a counting system

passers-by where, through the use of so-called "smart cameras",

passers-by are filmed and where the relevant video images are then stored locally

temporarily (i.e. for less than 1 second), only to be scrambled and

sent to the data center of the subcontractor.

31. On the basis of the foregoing, the Litigation Chamber finds that in this case, it is

question of processing of personal data within the meaning of article 4.1 juncto

article 4.2 of the GDPR and that the Data Protection Authority is therefore

competent to control this processing and the Litigation Chamber to take a

decision on the matter.

2.2.

Identification of the data controller (article 4.7 of the GDPR)

32. In accordance with Article 4.7 of the GDPR, the person responsible for the

processing: the "natural or legal person, public authority, agency or other

body which, alone or jointly with others, determines the purposes and means of the

processing".

1 Directive 95/46/EC, repealed and replaced by the GDPR.

2 CJEU judgment of 11 December 2014, Ryneš, C-212/13, ECLI:EU:C:2014:2428, recitals 20-22 (underlining by the Chamber

Litigation).

33. The Court of Justice has on several occasions interpreted the concept of "controller"

broadly in its case law in order to ensure effective and comprehensive protection

of the persons concerned.3

34. In accordance with Group Opinion 1/2010 29, the quality of the data controller(s)

concerned must be concretely assessed.4

35. In the present case, the Litigation Division first notes that the defendant carried out a

processing of personal data within the meaning of Article 4.2 of the GDPR, namely "any

operation or set of operations whether or not carried out using automated processes and

applied to personal data or sets of data, such as

collecting, recording, organizing, structuring, storing, adapting, or

modification, extraction, consultation, use, communication by transmission,

dissemination or any other form of making available, reconciliation or interconnection,

limitation, erasure or destruction". As explained above, the Respondent processes

video images of passers-by, taken using cameras The fact that this processing is not

performed only for a short time does not alter the fact that it falls within the scope

GDPR material. It is indeed in this case a "automated processing in whole or

in part" within the meaning of Article 2 of the GDPR.

36. Still according to Opinion 1/2010 of the Group 29, the notions "ends" and "means" must

be examined together in an inseparable manner and in this respect it is necessary to establish who

determines the "why" (the purposes) and the "how" (the means) of the processing.5

37. The Litigation Division further notes that the defendant defined the purposes and

means of the processing of personal data concerned, given that the latter has issued

as a contracting authority, the public service contract having as its object "Metering

passers-by at specific locations on the dike and in shopping areas at the

Coast", specifying the purposes and means of the processing in question.

38. In addition, a subcontract was concluded between the defendant and the subcontractor on

June 17, 2020, in accordance with Article 28 of the GDPR, in which the first is designated

3 See in particular CJEU, 5 June 2018, C-210/16 - Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, recitals

27-29.

4 See Group 29, Opinion 1/2010 on the notions of "controller" and "processor", 16 February 2010 (WP 169),

as specified by the DPA in a note "Update on the notions of controller / processor with regard to

of Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal da

personnel (GDPR) and some applications specific to liberal professions such as lawyers".

5 Group 29, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, p. 15.

as being the data controller.6 The respondent also acknowledges

be the data controller.

39. Based on the foregoing, the Litigation Chamber concludes that the defendant must be

considered as data controller within the meaning of article 4.7 of the GDPR for the

processing of personal data under investigation. Considering the principle of

responsibility provided for in Articles 5.2 and 24 of the GDPR, it is therefore, in this

quality, required to ensure compliance with the principles and provisions of the GDPR.

2.3.

With regard to the findings of the Inspection Service in the context of serious indications

40. The Litigation Chamber notes that findings B.1 and B.2 of the Inspection Service

concern the legality of the system of counting passers-by using cameras

intelligent as such, while the other findings within the framework of the indices

seriously concern the privacy statement and the impact assessment relating to the

Data protection. The Litigation Chamber will examine

findings

mentioned above separately.

2.3.1. Compliance with the principles relating to the processing of personal data

(Articles 5.1 and 5.2 of the GDPR) and the lawfulness of the processing (Articles 6.1 of the GDPR)

41. In its findings B.1 and B.2, the Inspection Service finds that the defendant did not

not sufficiently demonstrated that the smart camera system used respects the

data protection principles. The Inspection Service declares more

specifically that the Respondent would have committed a violation of Articles 5.1 a) (lawfulness, loyalty

and transparency), 5.1 b) (purpose limitation) and 5.1 c) (data minimization) of the

GDPR as well as Articles 5.2 (responsibility) and 6.1 (lawfulness of processing) of the GDPR.

42. With regard to the aforementioned findings of the Inspection Service, the Chamber

Litigation draws attention to the fact that the use of so-called smart cameras in

the public space does not comply with the standards of European law in terms of the protection of

data only if and insofar as the following principles are respected:

6 According to the defendant's documents.

A. The processing of personal data via the camera system

intelligent data must be based on a valid reason for lawfulness within the meaning of Article 6 of the GDPR

Decision on the merits 24/2021 - 12/44

43. As with any processing of personal data, the processing of personal data

personal data by means of smart cameras is first of all lawful

if it takes place in accordance with

Article 6.1 of the GDPR and in particular if

and provided that at least one of the following conditions is met:

a) "the data subject has consented to the processing of his or her personal data

for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is

party or the execution of pre-contractual measures taken at the latter's request;

c) processing is necessary for compliance with a legal obligation to which the controller

processing is submitted;

d) processing is necessary to protect the vital interests of the data subject

or another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or falling within the

the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller

processing or by a third party, unless the interests or freedoms and rights

fundamentals of the data subject which require data protection to be

personal character, in particular when the data subject is a child."

44. If special categories of personal data - such as personal data

relating to the health of data subjects - are processed via the system, the person responsible

of the processing must also demonstrate that one of the grounds for exception of Article 9.2 of the GDPR

applies. In this case, however, this has not been demonstrated.

45. In accordance with Guidelines 3/2019 on the subject of the European Committee on

data protection (hereinafter referred to by the English abbreviation: "EDPB"), in principle

any legal basis provided for in Article 6.1 of the GDPR may constitute a legal basis

for the processing of personal data obtained via video images. The EDPB

clarifies, however, that in practice such processing will generally be based on

GDPR Article 6.1 f) (legitimate interest) or GDPR Article 6.1 e) (necessary to

performance of a task in the public interest or in the exercise of official authority).

Decision on the merits 24/2021 - 13/44

In rather exceptional cases, Article 6.1 a) GDPR (consent) can be used

as a legal basis by the controller.7

46. In the present case, it appears from the submissions in response of the Respondent, from the register of the activities of

treatment held by the latter as well as the impact analysis relating to the protection of

data he has made that he bases the processing of personal data on

question on article 6.1 e) of the GDPR. The Respondent more specifically states that its

mission of public interest consists in supporting and promoting tourism in West Flanders

and specifies that this implies that this tourism can be done in complete safety. It refers to

in this regard to the management contract concluded with the province of West Flanders for the period

2020-2024.8 The defendant specifies that the system for counting passers-by by means of

smart cameras was intended to fight the Covid-19 pandemic and preserve

the safety of visitors to the Coast.

47. The Litigation Chamber emphasizes that recourse to the ground of lawfulness set out in Article 6.1 e)

of the GDPR implies that the controller must be able to demonstrate that:

i)

the latter is entrusted with a mission of public interest or relating to the exercise of authority

public; and

ii)

the processing in question is necessary for the performance of the task□

above (see also point B below).□

48. With regard to point (i), recital 45 of the GDPR and Article 6.3 of the GDPR clarify□

that processing based on Article 6.1 e) of the GDPR "should have a basis in the law□

of the Union or in the law of a Member State". The GDPR thus excludes a "mission of interest□

public" or "relating to the exercise of public authority" is entrusted to the head of the□

treatment under a contract, even if the contract was concluded in the public interest9.□

49. With regard to this basis that processing based on Article 6.1 e) should have "in□

Union law or in the law of a Member State", recital 45 of the GDPR adds in□

besides this:□

7 EDPB, Guidelines 3/2019 (version 2.0) on the processing of personal data by video devices,□

available via this link: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-□

personal-data-through-video_en (hereinafter Guidelines 3/2019), point 16.□

8 Defendant's Exhibits.□

9 KOTCHY, W., “Article 6. Lawfulness of processing” in KUNER, C., BYGRAVE, L.A. and DOCKSEY, C., The EU General Data

Protection Regulation (GDPR). A commentary, Oxford University Press, Oxford, p. 335.□

“It should also be a matter for Union law or the law of a Member State to□

determine the purpose of the processing. Furthermore, this law could specify the conditions□

of this Regulation governing the lawfulness of the processing of personal data□

personnel, establish the specifications aimed at determining the data controller, the type□

of personal data being processed, data subjects,□

entities to which the personal data may be communicated, the□

purpose limitations, retention period and other measures to ensure a□

lawful and fair processing. It should also be part of Union law or the law of a□

Member State to determine whether the controller carrying out a task of interest□

public or subject to the exercise of public authority should be a public authority or a

other natural or legal person governed by public law (...) ”[Emphasis by the Chamber

Litigation].

50. Recital 45 of the GDPR clarifies, however, that a specific legal provision is not

required for each individual treatment. Legislation serving as a basis for

several processing operations which are necessary for the performance of a task in the public interest

or falling within the exercise of official authority may therefore suffice.

51. In the present case, the data controller refers to the management contract concluded with

the province of West Flanders as a basis for its mission in the public interest within the meaning of

Article 6.1 e) of the GDPR and for its mission described in this contract (see above). In his

impact assessment relating to data protection10, the respondent specifies that "the basis

legal basis for this processing is within the tasks of public interest and public authority

local authorities”11.

52. The Litigation Chamber draws attention to the fact that one of the public interest missions

of local authorities (i.e. municipalities) consists in guaranteeing the security of

people on their territory (see in particular article 135, § 2 of the New municipal law).

It notes that, in the present case, the defendant does not however mention what is the

precise legal basis in European law or Belgian law which justifies the disputed processing.

53. In accordance with Article 6.3 of the GDPR, as already “indicated, "the purpose of the processing must

be defined in this legal basis or, with regard to the processing referred to in

10 Defendant's Exhibits.

11 Respondent's DPIA, p. 5.

paragraph 6.1, point e), it must be necessary for the performance of a task in the public interest or

in the exercise of official authority vested in the controller".

54. Furthermore, according to Article 6.3 of the GDPR, the legal basis may also

"contain specific provisions to adapt the application of the rules of this

Regulation, inter alia: the general conditions governing the lawfulness of the processing by the

controller; the types of data that are subject to processing; the people

concerned; the entities to which the personal data may be transferred

communicated and the purposes for which they may be communicated; purpose limitation;

retention periods; and processing operations and procedures (...)".

55. In this respect, the Litigation Chamber also refers to the opinions on the legislation of

the Data Protection Authority (Knowledge Center) - e.g. regarding

certain measures taken as part of the fight against the spread of the coronavirus on

the basis of Article 6.1 e) of the GDPR - in which it is also pointed out that in accordance

to the aforementioned Article 6.3 of the GDPR, read together with Article 22 of the Constitution and

Article 8 of the ECHR, a standard of legislative rank must determine the characteristics

essential for the processing of data necessary for the performance of a task in the public interest

or in the exercise of official authority vested in the controller.

In the aforementioned notices, it is emphasized in this respect that the processing in question must

be framed by a standard that is sufficiently clear and precise and whose application is

predictable. for the people concerned. In this context, it is specified that this standard

must include the following elements in particular: the specific purpose(s) of the

processing ; the identity of the controller(s); data categories

processed, it being understood that these must prove – in accordance with article 5.1 of the GDPR,

"adequate, relevant and limited to what is necessary in relation to the purposes for

which they are processed"; the categories of data subjects whose data

will be processed; the data retention period; the recipients or categories of

recipients to whom their data is communicated and the circumstances in which

and the reasons for which they will be communicated as well as the possible limitation of the

obligations and/or rights referred to in Articles 5, 12 to 22 inclusive and 34 of the GDPR.12

56. In this respect, the Litigation Chamber nevertheless emphasizes that the missions of public interest or

in the exercise of official authority vested in controllers

are often not based on circumscribed legislative obligations or standards with

precision meeting the requirements mentioned in point 55, more precisely the definition

12

(https://www.autoriteprotectiondonnees.be/citoyen/chercher).

36/2020,

See

opinion

a.o.

the

42/2020,

44/2020,

52/2020

and

64/2020

essential characteristics of data processing. Rather, the treatments are carried out

on the basis of a more general authorization to act to the extent necessary to

accomplishment of the mission - such as, in this case, the safety and health of

inhabitants and tourists in the coastal municipalities.13 This is often legislation

relatively old where the aspect of data protection has not yet been

sufficiently developed. It follows that in practice the legal basis in question does not

often contains no provision concretely describing the data processing

required. Data controllers who wish to invoke Article 6.1 e) of the GDPR

on the basis of such a legal basis must then themselves carry out a weighting between

the necessity of the processing for the mission of public interest and the interests of the persons
concerned.
57. In the present case, the Litigation Chamber therefore finds that the defendant demonstrates
plausible way that he pursues a mission of public interest within the meaning of Article 6.1 e) of the
GDPR. However, it should be noted that the defendant himself does not indicate on what
specific legal basis (such as Article 135, § 2 of the New Municipal Law) in law
of the Union or the law of a Member State within the meaning of Article 6.3 of the GDPR the processing activity
in question - namely the processing of personal data via a system of
smart cameras in the fight against Covid-19 - is founded.
58. It is obviously incumbent in the first place on the public authorities at whose request the
processing takes place - in this case the province of West Flanders and the coastal municipalities
concerned - to ensure that there is a legal basis which meets the requirements of Article
6.3 GDPR. This does not preclude that it is also the responsibility of a data controller
such as the defendant to verify to what extent there is a sufficient legal basis.
59. In this decision, the Litigation Division limits itself to these general considerations
about the legal basis. It did not examine the presence of a legal basis
ad hoc for the processing in question by Westtoer. She draws attention to the fact that a
full analysis of the legal basis would also require involving the province
as well as all the municipalities concerned. This would greatly increase the
complexity of the analysis by the Litigation Chamber. Given the great societal importance of a
timely decision of the Litigation Chamber which sets strict conditions in
view of possible future counts of passers-by, this analysis was not carried out in the
framework of this decision.
13 KOTCHY, W., “Article 6. Lawfulness of processing” in KUNER, C., BYGRAVE, L.A. and DOCKSEY, C., The EU General Dat
Protection Regulation (GDPR). A commentary, Oxford University Press, Oxford, p. 336.

60. The Litigation Chamber nevertheless emphasizes that for any processing activities

future similar cases, the respondent and other controllers must ensure that

that the conditions of Article 6.1 e) of the GDPR juncto Article 6.3 of the GDPR are met,

in accordance with the liability set out in article 5.2 of the GDPR. In a future decision

concerning measures in the context of the health crisis, the Litigation Chamber may

also examine the correctness of the legal basis.

B. The necessity and proportionality of the measure must be demonstrated in relation to

for the purposes targeted by the use of smart cameras

61. In addition to the requirement that the processing of personal data by means of cameras

intelligence can only take place with a valid reason for lawfulness, it is appropriate

in addition to demonstrate that the use of the system is necessary (ii; see point above

47) and that this does not involve a disproportionate infringement of the right to data protection

of the persons concerned. This requirement of necessity appears in several provisions of the

GDPR, in particular Article 5.1 c) (data minimization principle) and Articles 6.1 c)

and 6.1 e) GDPR.

62. The necessity and proportionality test is even more important if the head of the

processing bases the processing concerned, as is the case here, on the latter

provision, Article 6.1 e) of the GDPR. Contrary to Article 6.1 c) of the GDPR (legal obligation

to which the controller is subject), the mission of public interest or falling within the

the exercise of official authority vested in the controller will not result in

indeed often not - as already indicated above - by obligations described with

precision, but rather by a more general authorization to act to the extent necessary to

accomplishment of the mission, such as in this case preserving the safety and health of

inhabitants and tourists of the Coast.14

63. It follows that the controller must, where appropriate, carry out a certain

balancing between the necessity referred to in the aforementioned article and the interests of the persons

concerned. In this regard, it should be emphasized, with regard to this weighting of the

interests, that Article 6.1 e) of the GDPR does not fundamentally differ in substance from

GDPR Article 6.1 f) (legitimate interest). The aforementioned element of weighting of interests

also explains the right to object set out in Article 21 of the GDPR, which only applies

for processing based on these two grounds of lawfulness.

14 KOTCHY, W., “Article 6. Lawfulness of processing” in KUNER, C., BYGRAVE, L.A. and DOCKSEY, C., The EU General Dat

Protection Regulation (GDPR). A commentary, Oxford University Press, Oxford, p. 336.

64. The Litigation Division draws attention to the fact that it is necessary to assess in particular the

necessity and that the weighting explained above must be carried out in the light of the

case law of the Court of Justice of the European Union as well as Article 8 of the

European Convention on Human Rights (ECHR) and Article 22 of the Constitution

Belgian, as well as the seriousness of the interference in the privacy of the persons concerned.

65. In its case-law - notably in the Huber judgment - the Court of Justice of the European Union

Commission points out in this respect that the concept of "necessity" within the meaning of Article 6.1 e) of the

GDPR should be interpreted strictly and assessed in light of proportionality and

that, in other words, if several alternatives exist to achieve the intended purpose, it

should opt for the least intrusive.15

66. The necessity and proportionality of the measure must therefore be more

precisely demonstrated with regard to the absence of less intrusive means for the rights

and freedoms of the persons concerned via which the intended purposes could also

be achieved.

67. With regard to the necessity of the smart camera system he uses, the defendant

affirms in its conclusions in response as well as during the hearing first of all that this

passers-by counting system was the only way to effectively fight against the

of the Covid-19 pandemic and therefore to accomplish its mission in the public interest, for the reasons

following:

i.

only counting via smart cameras can provide data

sufficiently precise on the number of visitors. The defendant clarifies in this regard that

visitor flows are complex and only the smart camera system

can measure such visitor flows with sufficient precision, whereas

alternative monitoring systems are much less accurate;

ii.

only counting via smart cameras can provide information

crucial extras. The Respondent states in this regard that in order to take

appropriate decisions, additional information should be obtained, such as

in particular the direction of visitor flows; and

iii.

that only counting via smart cameras allows real-time reporting

necessary. The defendant specifies in this respect that in order to be able to intervene

immediately if necessary, it is necessary to be able to make a report in time

real and that only the intelligent camera system allows the display of the affluence

on a real-time dashboard and sending push notifications.

15 CJEU, Huber, C-524/06, ECLI:EU:C:2008:724, par. 59-61.

68. The Respondent points out that the same result could not be achieved by using

alternative monitoring systems, such as manual counts or measurements via

Wi-Fi signals, as these are not precise enough for the purpose

intended and that only the system used makes it possible to obtain certain additional information

necessary to achieve this purpose. The Respondent specifically asserts that the

compliance or not with the rules of social distancing, the direction of movement of passers-by and

different types of passers-by - such as cyclists and pedestrians - cannot be

observed by any alternative system and that only the smart camera system allows

a real-time report, which is crucial in order to be able to communicate and, if necessary,

intervene in a timely manner.

69. With regard to the proportionality of the relevant processing activity, the respondent

points out that the processing takes only a fraction of a second, since the images from the cameras

filmed live are almost immediately anonymized and transformed into raw data

(aggregated counting data) and in images scrambled by the software (locally on the camera

same). The defendant insists that the live images are then only stored

anywhere but are immediately deleted from the camera's memory.

70. The Respondent also draws attention to the fact that the proportionality of the measure

is also guaranteed by its limitation in time and space. He specifies

firstly in this respect that the contract with the subcontractor was deliberately concluded for

a short period of three months and that the measure was therefore only applicable

during this period (i.e. the summer period). Second, it highlights the choice

deliberated on the places where the smart cameras in question have been installed and specifies that it

these were only places where a particular crowd was expected (i.e.

dykes and shopping streets).

71. Based on the foregoing, the Litigation Chamber considers that the Respondent demonstrates

the necessity and proportionality of the system concerned with a view to achieving the purposes

targeted. The defendant indeed demonstrates the absence of an alternative system - less intrusive -

which could achieve these ends in the same way. He also demonstrates having taken the

necessary measures to ensure proportionality (see also below).

C. Data protection by design and data protection by default

(Article 25 GDPR)

72. When processing personal data by (smart) cameras, it is

crucial - given the potentially significant risks to the rights and freedoms of individuals

concerned - that the controller takes appropriate measures to ensure

that the principles of data protection are integrated in a way

effective so that the risks of violation of the rights and freedoms of the persons concerned

be limited as much as possible.

73. The "appropriate measures" mentioned above are not only technical in nature

but also organizational and must be taken by the data controller before the

start of processing activities such as, in this case, the collection of video images, namely

when determining the purposes and means of processing.16

74. In other words, the data controller must respect the principles of 'data

protection by design' ('data protection by design') and 'data protection

by default'.17

75. These concepts constitute one of the cornerstones of the GDPR and the accountability principle.

of article 5.2 juncto article 24 of the GDPR, which occupies a central position there. They are taken

in Article 25 of the GDPR and are specified in recital 78 of the GDPR.

76. In accordance with Article 25.1 of the GDPR, "Taking into account the state of knowledge,

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

processing as well as the risks, of varying likelihood and severity, that

processing for the rights and freedoms of natural persons, the controller

implements, both at the time of determining the means of processing and at the time

the processing itself, appropriate technical and organizational measures, such as

pseudonymization, which are intended to implement the principles relating to the

data protection, e.g. data minimization, effectively and to

attach the necessary safeguards to the processing in order to meet the requirements of the GDPR and

to protect the rights of the data subject".

77. Article 25.2 of the GDPR provides that "The controller shall implement the
appropriate technical and organizational measures to ensure that, by default, only
the personal data that is necessary for each specific purpose
of processing are processed. This applies to the amount of personal data
collected, the extent of their processing, their retention period and their accessibility.
In particular, these measures ensure that, by default, personal data
are not made accessible to an indeterminate number of natural persons without
the intervention of the natural person concerned".

16 Guidelines 3/2019, point 126.

17 The Litigation Chamber will hereafter use the abbreviation "DPbDD" when it concerns both concepts simultaneously.

78. Recital 78 of the GDPR specifies with regard to the technical measures and
above-mentioned organizational structures that they "could consist, among other things, of reducing to a
minimum the processing of personal data, to pseudonymize the data to be
personal nature as soon as possible, to ensure transparency with regard to the
functions and the processing of personal data, to allow the person
data subject to control the processing of data, to allow the controller
to put in place or improve security measures".

79. In its DPbDD Guidelines 4/2019, the EDPB clarifies that the protection of
default data refers to a pre-existing or preset value of an adjustable parameter
within a software application In these Guidelines, the EDPB describes the protection of
data by design as having the objective of "protecting the rights of individuals
concerned and to ensure that the protection of their personal data is proper
('integrated') into the treatment".18

80. In its case-law, the Court of Justice has also underlined the importance of these concepts
and notably asserted in its Digital Rights Ireland judgment that the essence of Article 8 of the

Charter of Fundamental Rights of the European Union requires the adoption of measures
technical and organizational to ensure that personal data is
effectively protected against any risk of misuse as well as against any access and
illicit use of this data.19
81. In the present case, the Litigation Chamber finds, on the basis of both the documents in the file and the
the demonstration of the smart camera system by the defendant during the hearing, that
the latter has taken a series of organizational and technical measures to limit the
maximum the processing of personal data on the one hand and to protect and
secure this data on the other hand.
82. These measures were taken after the opinion of the Data Protection Officer and after
carrying out a data protection impact assessment on the basis of Article
35 GDPR by the defendant regarding the smart camera system
(see also points 131 e.s.).
83. The Litigation Division also finds that the defendant integrated the protection of
personal data ab initio in the implementation of the project. It stands out
18 EDBP, Guidelines 4/2019 (version 2.0) on data protection by design and by default of article 25 of the
GDPR,
:
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
(hereafter: Guidelines 4/2019).
available
the address
at
19 ECJ, Joined Cases C 293/12 and C 594/12, Digital Rights Ireland, para. 40 and 66-67.

in particular due to the fact that in the special specifications entitled "Counting of passers-by at

specific places on the dyke and in shopping areas at the Coast" by which

the latter issued the public contract for the implementation of the aforementioned system, the

contractual provisions included a title concerning the processing of data and the

compliance with the provisions of the GDPR by the tenderer, who acts as a subcontractor

Datas. During the hearing, the defendant clarified that the final tenderer

in particular was selected because of the particular attention it paid to the protection

personal data. The defendant thus acts in accordance with the prescription of the

recital 78 of the GDPR, in fine, which states on this subject that "The principles of protection of

data-by-design and default data protection should also be

taken into account in public procurement".

84. It appears from the documents in the file as well as from the defendant's oral defense that when

actual implementation of the system by the defendant and the subcontractor, a series of

technical and organizational measures have also been taken for the protection

personal data, in accordance with Articles 25.1 and 25.2 of the GDPR.

85. The first article cited mentions among these technical and organizational measures to be

be taken by the data controller first of all the pseudonymization of the data

of a personal nature in question. Recital 78 of the GDPR also mentions that

"These measures could consist, inter alia, [...] in pseudonymising the data to be

personal character as soon as possible".

86. According to the documents in the file and the demonstration of the intelligent camera system

made by the defendant to the Litigation Chamber during the hearing, the Chamber

Litigation understands that the passer-by counting system in question includes a

software component and a hardware component, associating each installed camera with a

printed circuit board ("PCB") operating as a local Single Board Computer in order to

locally process the images in real time. The camera images (frames) are processed in

local, on site ("on premise"), by the PCB.

87. The demonstration of the system during the hearing shows that the cameras in question film

indeed passers-by, but that in a fraction of a second, the relevant objects (such as

bicycles and cars) as well as individual persons are distinguished and replaced

by what is called a "blob". This is a colored box that represents a passerby or

a recognized object. Filmed passers-by are therefore analyzed in real time by the intelligence

machine and a self-learning algorithm.

Decision on the merits 24/2021 - 23/44

88. In its Guidelines 3/2019, the EDPB has also underlined in this respect that, applied

to the processing of personal data by means of video devices, examples

such privacy-friendly technologies within the meaning of Article 25 of the GDPR are the

systems that make it possible to mask or blur irrelevant areas or to

remove images representing third parties as part of the transmission of footage

video to those concerned.20

89. The defendant explains in this regard - in particular with the help of screenshots of the cameras in

question - only in a first phase, namely during the first hour following

installation of these cameras, we film at low resolution (image 1) and then, in a

second phase, users are replaced by "blobs" (also called "images

scrambled" in this Decision). The Respondent clarifies that the (brief) treatment of these

images is only done locally - more precisely on the same installed camera - and

that then, two data streams go from these devices to the data center of the

subcontractor, namely (i) the scrambled images and (ii) the aggregate counting data.

These latest data make it possible to measure attendance - and to control the rules of

social distancing - and to intervene if necessary. According to the documents in the file and the

explanations provided by the defendant, the images of the cameras themselves are not

stored nowhere.

Figure 1. Low resolution images displayed by the firmware (phase 1)

20 Guidelines 3/2019, point 129.

Figure 2. Users replaced by "blobs" (phase 2)

90. Based on the foregoing, it appears that the images from the cameras in question are

almost immediately anonymized and that the identification of passers-by filmed is made

impossible.

91. The Litigation Chamber considers that this meets the requirements of Article 25.1 of the GDPR and

of recital 78 of the GDPR as well as the principle of data minimization set out in Article

5.1 c) of the GDPR, to which reference is also made by the first provisions mentioned.

While Article 25.1 of the GDPR only requires pseudonymisation, the data to be

personal character in question are irreversibly anonymised.

92. Thanks to this almost immediate anonymisation, only data

of a personal nature which are "relevant" and "limited to what is necessary with regard to

of the purposes for which they are processed" and these are then converted into data

anonymous counting as well as scrambled images.

93. The measures described above also make it possible to meet the requirement of Article

25.2 of the GDPR according to which the data controller must guarantee that "by default, only

the personal data that is necessary for each specific purpose

processing is processed", which applies to "the amount of personal data

collected, the extent of their processing, their retention period (...)". Both the quantity

of personal data than the retention period for live images - which is

of only a few milliseconds - are thus limited to a minimum, which makes it possible to

respect the principle of limitation of storage (art. 5.1 e) of the GDPR.

94. It appears from the documents in the file that the Respondent also took several other measures

technical and organizational in order to limit as much as possible the processing of data to

personal character, more specifically:

i.

the limitation of the measurement in space, namely the placement of smart cameras

only in places where there is a risk of large crowds (for example

dykes and shopping areas);

ii.

limitation of the measurement in time: the passers-by counting system at the

means of smart cameras was used from June 2020 until September 30, 2020,

and this with the exception of a single municipality, where due to the constant influx,

the use of the system has been extended until February 1, 2021; and

iii.

limiting and securing access to camera images (see below).

95. Article 25.2 in fine of the GDPR provides with regard to this last aspect that the accessibility

of the personal data in question must be limited, in particular to guarantee

that "by default, personal data [are] not made accessible to a

indefinite number of natural persons without the intervention of the natural person

concerned".

96. The Litigation Chamber also refers in this regard to Guidelines 3/2019 of the

the EDPB in which the latter emphasizes the importance of the security of the

system and data and states that it refers to "the physical security of

all the components of the system and to the integrity of the latter, i.e. the protection

and resilience against any interference, intentional or not, in its functioning

normal and access control" as well as "confidentiality (the data is only accessible

only to persons with a right of access), integrity (prevention against the loss or

manipulation of data) and availability (the data is made accessible as soon as

that it is necessary)".21

97. In this regard, the Litigation Chamber finds on the basis of the documents in the file that the
responsible for the processing as well as the subcontractor have taken the technical and
organizational measures necessary to guarantee the security of the data and limit access to them.
here exclusively to authorized persons.
98. In its submissions in response, the Respondent states more specifically in this regard that
only a limited number of employees (i.e. seven) of the subcontractor have access to the images
live scrambled (and therefore in principle anonymous) which are transferred to the date center of the
subcontractor for the sole purpose of controlling the proper functioning of the system
(for example: check if the lens of the cameras is clean and if the cameras are well
positioned).
21 Guidelines 3/2019, point 132.

99. The defendant further demonstrates that access to these images is subject to security measures.
strict security and is subject to tracing. During the hearing, the defendant specifies on this subject
that authorized employees only have access to images from the data center, that
multiple passwords are required to gain access to these images and that access is
limited to fifteen minutes. The Respondent also pointed out in this matter that neither the
participating municipalities, nor himself have access to the live images of the cameras. He has
added that he himself only saw these (blurred) images for the first time in preparation
hearing in these proceedings. These scrambled live images are only
further stored nowhere.
100. With regard to the technical and organizational measures prescribed by Article 25
of the GDPR, the EDPB also underlines in its Guidelines that the solutions chosen do not
should not offer superfluous features (such as unlimited motion cameras
or having zooming, radio transmission or analysis and recording capability
sound). The EDPB adds to this that the functions provided but which are not necessary

must be deactivated.22

101. The defendant clarifies in this respect that in the firmware of the camera system concerned

intelligent, the functions that are not necessary for the purpose pursued have been

deactivated. He further specifies that, for example, it has been made impossible to deactivate the

jamming applied. The defendant adds that the artificial intelligence software does not allow

not technically get unscrambled live images from smart cameras and

it refers in this respect to a written declaration of the subcontractor on the matter.

102. The Litigation Chamber draws attention to the essential importance of the measures

aforementioned techniques to ensure that the images cannot be used for

incompatible manner for purposes other than those for which the data was

collected (for example making the data accessible to third parties such as law enforcement

order), which would be contrary to the principle of purpose limitation set out in Article 5.1 b)

of the GDPR.

103. Based on the foregoing, the Litigation Chamber concludes that, in accordance with the

liability incumbent on it under Article 5.2 juncto Article 24 of the GDPR, the defendant

demonstrates that from an early stage of the project treatment activities through

the use of the smart camera system, it took the technical measures and

appropriate organizational measures necessary to guarantee from the outset compliance with the principles in

22 Guidelines 3/2019, point 129.

privacy and data protection. The system put in place by the

defendant therefore constitutes a good example of "data protection by design" ("protection of

data by design") within the meaning of Article 25 of the GDPR.

104. The defendant demonstrates in particular that from the issuance of the public contract relating to the system

counting passers-by, he took into account compliance with the above-mentioned principles by

considering technologies that meet the requirements of the DPbDD. He has

opted for a 'stand alone' system, not connected to any network, where the

processing of personal data by means of a video device is limited to the

minimum and where no other personal data is collected.

105. The Respondent provided an appropriate management framework and took technical measures

regarding the (intended) processing, more specifically regarding:

i.

anonymisation, in accordance with Article 25.1 of the GDPR and recital 78 of the

GDPR, thanks to the automatic and irreversible "scrambling" of camera images

after a few milliseconds by replacing the pedestrians with "blobs";

ii.

data minimization (Art. 5.1 c) of the GDPR, thanks to the retention period

short and to the limitation of the measurement in time and space;

iii.

retention limitation, by not retaining camera images anymore

longer than what is strictly necessary for the achievement of the intended purposes

(local recording for only a few milliseconds) and retaining

data obtained in a form that makes it impossible to re-identify the

data subjects, in accordance with Article 5.1 e) of the GDPR;

iv.

data security and access limitation, by limiting access to images by

direct scrambled to a limited number of employees of the subcontractor authorized for this

effect (even when the people in these scrambled live images cannot

principle not be re-identified), the security of access to the system thanks to several

passwords as well as access tracking and also its time limitation

;

v.

disabling superfluous features in the system firmware

so that no unscrambled live image that would allow identification

of the persons concerned cannot be extracted from the cameras and that it is

technically impossible to disable automatic image scrambling.

106. The defendant has thus fulfilled the requirements of Article 25 of the GDPR. Bedroom

Litigation takes into account the fact that the current health crisis requires the adoption of

exceptional measures which may require the processing of personal data

personnel in the general interest, such as, for example, the fact of filming movements of

Decision on the merits 24/2021 - 28/44

people. In this context, it is essential that a data controller takes the

maximum precautions to limit the harmful consequences to a minimum

potential for the data subjects whose data are processed.

107. Based on the foregoing, the Litigation Chamber also concludes that the defendant

has not violated Articles 5.1 a), 5.1 b) and 5.1 c) of the GDPR and that the latter has sufficiently

demonstrated to have complied with data protection principles when deploying the

passers-by counting system.

2.3.2. Transparency of information and communications and procedures for exercising

rights of the data subject (Articles 12 and 13 of the GDPR)

108. In its investigation report, the Inspection Service notes that the declaration of

confidentiality of the defendant on the website www.westtoer.be/nl/dataverwerking23 does not

does not meet the transparency obligations of Articles 12.1, 12.6, 13.1 and 13.2 of the GDPR.

109. The Inspection Service firstly finds in this respect a violation of Articles 12.1 and

12.6 of the GDPR, in particular given the fact that:

1)

the information that is provided to the data subjects via the declaration of

confidentiality are not completely correct and are therefore not transparent, given

that it is not mentioned what changes have been made to this statement of

confidentiality or when;

2)

the lawful ground on which the respondent is processing the personal data

data subjects is not mentioned in a transparent manner;

3)

the privacy statement erroneously states that the personal data

processed for statistical study purposes are pseudonymised, which would mean, depending on the

defendant that the data cannot be linked to an individual;

4)

the defendant's privacy statement incorrectly states that a data subject

who wishes to exercise their rights must first contact the Data Controller and

wait for his response before sending his request to the Data Protection Officer;

5)

the privacy statement mentions that for the exercise of the rights of persons

concerned, a copy of the identity card is requested by the defendant, which would be

disproportionate; and

6) with regard to the possibility for data subjects to lodge a complaint

with a supervisory authority, the privacy statement refers only to

23 Screenshots of which were taken by the Inspection Service on July 13, 2020 and July 18, 2020.

Decision on the merits 24/2021 - 29/44

the Belgian Data Protection Authority, while Article 77.1 of the GDPR provides that a

complaint can be lodged with any European supervisory authority.

110. In addition, the Inspection Service finds a violation of Articles 13.1 and 13.2 of the GDPR,

seen that :

1)

the precise purposes and the legal basis of the processing are not mentioned in the

Confidentiality declaration ;

2)

the retention periods or the criteria used to determine these periods are not

mentioned; and

3)

the right for data subjects to withdraw the consent given for the use

of cookies is not mentioned.

111. During the hearing, the Respondent acknowledges that the Privacy Statement has been adapted

belatedly, but he specified that he had above all concentrated on the impact analysis relating to the

data protection as well as the lawfulness of the system itself. The defendant

adds to this that the privacy statement has been amended in the meantime, following and

in accordance with the findings of the Inspection Service, and he points out that an adviser

has been appointed to further adapt, if necessary, the documents relating to

privacy from mid-January 2021.

112. The Litigation Chamber draws attention to the fact that in accordance with Article 12.1 of the

GDPR, the controller "[takes] appropriate steps to provide any

information referred to in Articles 13 and 14 as well as to carry out any communication to the

under Articles 15 to 22 and Article 34 with regard to personal processing

concerned in a concise, transparent, comprehensible and easily accessible manner, in

plain and simple terms (...)".

113. Recitals 58 and 60 of the GDPR specify that "The principle of fair and

transparent requires that the person concerned be informed of the existence of the operation of

processing and its purposes" and that "The principle of transparency requires that any information

addressed to the public or the data subject is concise, easily accessible and easy to

to understand (...)".

114. In the event that the personal data in question were not collected from

of the data subject himself, Article 13 of the GDPR prescribes which information

must be provided to the latter:

Decision on the merits 24/2021 - 30/44

“Where personal data relating to a data subject is

collected from this person, the data controller provides him, at the time when

the data in question are obtained, all of the following information:

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

representative of the controller;

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

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

the legal basis for the processing;

d) where the processing is based on Article 6(1)(f), the legitimate interests

sued by the controller or by a third party; (e) the recipients or the

categories of recipients of personal data, if any; and

f) where applicable, the fact that the controller intends to make a transfer

personal data to a third country or to an international organisation, and

the existence or absence of an adequacy decision issued by the Commission or, in the case

transfers referred to in Article 46 or 47, or in the second subparagraph of Article 49(1), the

reference to the appropriate or adapted safeguards and the means of obtaining a copy or

where they were made available.

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

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

following additional information that is necessary to ensure processing

fair and transparent:

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

possible, the criteria used to determine this duration;□

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

personal character, the rectification or erasure of these, or a limitation of the□

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

data portability;□

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

paragraph 2(a), the existence of the right to withdraw consent at any time, without□

undermine the lawfulness of processing based on consent made prior to withdrawal□

of it; d) the right to lodge a complaint with a supervisory authority;□

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

personnel is of a regulatory or contractual nature or if it conditions the conclusion of a□

contract and whether the data subject is obliged to provide the personal data,□

as well as on the possible consequences of not providing this data;□

f) the existence of automated decision-making, including profiling, referred to in Article 22,□

paragraphs 1 and 4, and, at least in such cases, useful information concerning the logic□

Decision on the merits 24/2021 - 31/44□

underlying data, as well as the significance and anticipated consequences of such processing for the□

concerned person".□

115. The Litigation Chamber consulted the defendant's confidentiality statement (latest□

consultation on 05/02/2021) and indeed noted on this occasion that it has□

has actually been adapted in such a way as to take into account the majority of the Service's remarks□

of inspection and that therefore the privacy statement has been almost□

fully compliant with the relevant provisions of the GDPR. Bedroom□

Litigation takes note of this.□

116. It should be noted, however, that not all the findings of the Inspection Service have yet been□

been taken into account.□

117. The Litigation Chamber notes first of all in this respect that the declaration of confidentiality does not mention in sufficient detail the basis(s) legal(s) for the processing of the personal data in question, as required Article 13.1 c) of the GDPR. The privacy statement mentions in particular in this respect :

"We process your personal data on the basis of either:

• your consent.

• a contract between us.

• a legal obligation with which we must comply.

• of public interest."

118. However, it is not specified which legal obligations or which public interest are involved. Thus, for example for the processing of personal data via the system of smart cameras, it is not specifically mentioned what is the legal basis for the processing in question (see above article 6.3 of the GDPR).

119. In accordance with the Guidelines on Transparency drafted by the Group 29, the information provided on the basis of Articles 13 and/or 14 of the GDPR must be concrete and final and may not contain any abstract or ambiguous formula. The Group 29 emphasizes that this applies in particular to the purposes and the legal basis of the processing. 24

24 Guidelines on Transparency within the meaning of Regulation (EU) 2016/679, WP260rev01, established on November 29, 20 9-10.

120. The Litigation Chamber considers that this constitutes a violation of Article 13.1 c) of the GDPR and therefore recommends to the defendant to specify this (these) legal basis(s) in accordance with the above provision.

121. Secondly, the Litigation Chamber finds that the declaration of confidentiality does not

nor does it clearly mention the retention periods for personal data

personnel concerned or the criteria for determining them, as required by Article

13.2 a) GDPR. The privacy statement mentions in this respect that "the data

are kept for as long as necessary to be able to offer our services, because

we have an interest in doing so or to fulfill our legal obligations".

of the Group Guidelines 29 that such wording is insufficient. The Group 29

emphasizes in this respect that the period / mention of the storage period is linked to the principle

minimization of the data set out in article 5.1, c) of the GDPR as well as the requirement of

retention limitation set out in Article 5.1, e) of the GDPR. He specifies that "The period of

conservation (or the criteria for determining it) can be dictated by different factors

such as regulatory requirements or industry guidelines, but should

be formulated in such a way that the data subject can assess, depending on the situation

in which it is located, what will be the retention period for personal data

specific or in the case of specific purposes.".25

122. The Litigation Chamber therefore recommends that the defendant further specify

the retention periods for the personal data collected in the declaration

of confidentiality, in accordance with Article 13.2 a) of the GDPR.

123. The Litigation Division further notes that the confidentiality statement mentions

the following regarding the exercise of data subject rights:

"We may need proof of your identity to be able to respond to your

request. In this case, we will ask you to provide a copy or scan of your card

identity or any other proof of your identity. We will use this evidence only

to establish that you are indeed the data subject whose personal data

staff are processed, or the parent or guardian for those under 16. As soon as we

we will both be satisfied with the answer to your question, we will destroy this evidence".

124. As also noted by the Inspection Service, the Litigation Chamber emphasizes that

in accordance with Article 12.6 of the GDPR, the controller may only

request additional information from the data subject "[when] there are

25 Group 29, Guidelines on transparency within the meaning of Regulation (EU) 2016/679, WP260Rev1, p. 45.

reasonable doubts as to the identity of the natural person making the request in question

in Articles 15 to 21". The systematic request for a copy or a scan of the card

identity of the data subject is therefore disproportionate.

125. The Litigation Division emphasizes in this respect that it is only in the specific cases where

in accordance with Article 5.2 of the GDPR, the controller is able to demonstrate

that he cannot identify this data subject (Art. 11.2 GDPR) and/or that he has

reasonable doubts as to the identity of the natural person making the request (Art.

12.6 of the GDPR) that he can request the additional data necessary to confirm

the identity of the data subject. This additional data can for example

consist of a copy of the front of the identity card where only the data to be read are

personal character which are strictly necessary for this verification. Others

data may have been previously rendered unreadable by the complainant.

126. The Litigation Chamber notes that the other findings of the Inspection Service have

have meanwhile been taken into account by the amendments made by the defendant to the

confidentiality statement, but notes however that they were drawn up at

the time when the inspection survey was carried out.

127. The Respondent acknowledges this and points out in its defence, as mentioned above, that it

primarily focused on GDPR compliance of the smart camera system

itself before adapting the privacy statement.

128. The Litigation Division nevertheless stresses the importance of respecting the obligations of

transparency on the part of a data controller from the start of the activity of

processing, given the impact this has on the exercise of the rights of data subjects set out

to Articles 15 to 22 inclusive of the GDPR, as illustrated by the case law of the Court of Justice.26

129. The Litigation Chamber further emphasizes that as an autonomous provincial authority

charged with a task of public interest, the defendant has an exemplary role in terms of respect

of the legislation relating to the protection of personal data and that by

Consequently, in accordance with the principle of "lead by example", he must ensure at all times that

act in accordance with this legislation and in particular to comply with the provisions

above GDPR transparency essentials.27

26 CJEU, 1 October 2015, Bara, C-201/14, ECLI:EU:C:2015:638.

27 Data Protection Authority, Strategic Plan 2020-2025",

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD_Plan_Strategique_28012020.pdf, p.

22.

130. Considering the cooperation of the defendant and the adaptation of the declaration of confidentiality during

of the procedure, the Litigation Chamber does not however consider it necessary to match the

above findings of a sanction, but nevertheless orders the defendant to

bring this privacy statement fully into compliance.

2.3.3. Data protection impact assessment (Articles 35.2 and 35.7 GDPR)

131. According to the Inspection Service, the defendant committed a violation of Articles 35.2 and 35.7

of the GDPR. The Inspection Service considers that the defendant did not collect, or in any event

not in time, the opinion of the Data Protection Officer on a DPIA (Article 35.2).

The Inspection Service further considers that the defendant did not comply with article 35.7

of the GDPR, which requires that the DPIA must contain the following elements: a) a description

systematic of the processing operations envisaged and the purposes of the processing,

including, where applicable, the legitimate interest pursued by the controller; b) a

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 individuals

concerned; d) the measures envisaged to deal with the risks, including guarantees,

security measures and mechanisms to ensure the protection of personal data

staff.

132. Respondent indicated in response to questions from the Inspection Service that the

data protection officer was involved from the outset in carrying out the DPIA

regarding smart cameras. According to the Respondent, the first consultation regarding

the DPIA took place on June 11, 2020. In the conclusions, the respondent repeats that both the delegate

to data protection that the respondent made it clear that the delegate had been

present and associated with the realization of the AIPD from the beginning on June 11, 2020. The Service

d'Inspection considers, however, that it has not been demonstrated that the above-mentioned consultation

actually took place and that the data protection officer was present. In

the opinion of the Data Protection Officer, reference is made to the DPIA with the terms

"the elaborate DPIA".28 According to the Inspection Service, the above indicates that the DPIA (at least

part of it) had already been drafted before the delegate gave his opinion. According to

the Inspection Service, it also lacks an assessment of the risks referred to in Article 35.1

of the GDPR for the rights and freedoms of data subjects (see Article 35.7 c) as well as

the measures envisaged to deal with the risks, including guarantees, measures and

security mechanisms to ensure the protection of personal data

(section 35.7d).

28 DPIA Notice from the Data Protection Officer Annex 5 via email dated July 28, 2020 from Respondent.

133. According to the Litigation Chamber, the documents presented do not allow

to establish that a discussion regarding the development of a DPIA took place on June 11, 2020 in

presence of the Data Protection Officer. In the absence of proof of the presence or

of the absence of the delegate, the Litigation Chamber cannot pronounce further on this

topic.

134. However, it is clear from the documents submitted that the Data Protection Officer
data from Westtoer provided its written notice (dated June 17, 2020) to Westtoer dated
June 18, 2020. In this opinion, remarks are made and the Data Protection Officer
AIPD approved data. According to Group 29, the controller must collect
the opinion of the data protection officer concerning a DPIA, in particular on the
following questions:
- what methodology should be followed when carrying out an impact assessment relating to the
Data protection ;
-
should the data protection impact assessment be carried out in-house or
be outsourced;
- what safeguards (including technical and organizational measures) must be applied
in order to mitigate possible risks to the rights and interests of persons
concerned;
-
whether the data protection impact assessment has been
correctly carried out and whether its conclusions (whether or not to proceed with the processing and
safeguards to be put in place) comply with the GDPR.29
135. The Litigation Chamber considers that in the written opinion of June 17, 2020 of the delegate for the
data protection, you can find a description of the possible risks that the
processing of data could entail as well as a description of the guarantees that may be
applied to counter them. The Data Protection Officer also indicated
in the notice that the DPIA meets the requirements of Article 35.7 of the GDPR and underlined therein that
the DPIA also took into account the points of attention described by the delegate in his opinion.
On June 25, 2020, therefore one week after the written opinion of the delegate, the DPIA was approved and
signed by the managing director and the president of the board of directors of the defendant. In view

of the foregoing as well as the grounds and supporting evidence invoked, the Litigation Division

therefore considers, unlike the Inspection Service, that the delegate for the protection of

data did issue an opinion on the DPIA. No violation of Article 35.2 of the GDPR

can be observed.

29 Group 29 WP 243 rev.01

Decision on the merits 24/2021 - 36/44

136. According to the Inspection Service, there are also violations of Article 35.7 c) and d)

of the GDPR. According to the Inspection Service, the DPIA contains too brief a description of the

risks to the rights and freedoms of data subjects. The DPIA would not show

how the risk assessment was carried out. The Inspection Service considers that the

measures envisaged to deal with the risks, including guarantees, measures and

security mechanisms aimed at ensuring the protection of personal data and

to demonstrate compliance with the GDPR have been described too briefly and too

insufficient.

137. The Litigation Division considers that the risks that the processing could generate

have been described and assessed with sufficient precision in the prepared DPIA. As the

Litigation Chamber has already noted it above in this decision, the defendant is

achieved both on the basis of a series of technical and organizational measures as well

that by limiting, protecting and securing as far as possible the processing of data

personal nature, to take the necessary measures against possible risks.

The Litigation Division therefore considers that no violation of Article 35.7 has been

committed.

2.4.

With regard to the findings of the Inspection Service outside the framework of the indices

serious

2.4.1. Consent to the placement of cookies (articles 4.11, 6.1 a), 7.1 and 7.3 of the GDPR)

138. The Inspection Service comes to the conclusion that the defendant is not asking for

consent for the placement of cookies on the website https://www.westtoer.be.

The Inspection Service finds a violation of Articles 4.11, 6.1 a) and 7.1 and 7.3 of the GDPR.

The screenshots of the aforementioned website taken by the Inspection Service on

13 July 201930 show that data subjects who visit the website

of Westtoer were deemed to have given their consent at the time they

continue browsing the site. This is the reason why it was not asked of the

prior to the persons concerned to give their consent for the use of cookies

on the website. Nor is consent required for the placement of

non-essential cookies. This is apparent from the sentence "By using this site or by clicking

on 'Approve', you consent to the use of cookies".

30 Exhibit 8 of the Inspection report of August 25, 2019

139. The notion of "consent" is made up of several elements which must be

cumulatively respected. Article 4.11 of the GDPR defines consent as:

"any manifestation of will, free, specific, enlightened and unambiguous by which the

data subject accepts, by a declaration or by a clear positive act, that personal data

of a personal nature concerning him or her are processed". The "free" element must

be construed as effectively offering a choice and leaving control of what

choice to the person concerned. Where a data subject has not actually had the

choice and feels compelled to give consent because the consequences

refusal would be detrimental, consent is deemed not to have been given

freely. If consent is a non-negotiable part of the terms,

considers that it was not freely given. This means that consent will not be

considered to have been given freely if the person concerned is unable to

refuse or withdraw consent without consequences.31

140. The Litigation Division refers in this respect32 to the Planet 49 judgment of the Court of Justice
European Union.33 In this judgment, the Court of Justice of the European Union clarified the requirement
of consent for the placement of cookies following the entry into force of the GDPR and
explained that explicit active consent was now required:
"Active consent is thus now expressly provided for by the Regulation
2016/679. It should be noted in this regard that, according to recital 32 of that regulation,
the expression of consent could be done in particular by ticking a box when
consultation of a website. That recital, on the other hand, expressly excludes that there
has consent "in case of silence, boxes checked by default or inactivity". He
it follows that the consent referred to in Article 2(f) and Article 5(3) of the
Directive 2002/58, read in conjunction with Article 4(11) and Article 6(1),
under a), of Regulation 2016/679, is not validly given when the storage
information or access to information already stored in the terminal equipment of
the user of a website is authorized by a box checked by default that the user
must uncheck to refuse consent." (Underlining by the Chamber
Litigation)
141. As described above, the Inspection Service noted on 13 July 2019 that visitors
of the website were supposed to have given their consent to the use of cookies as soon as
when they decide to continue browsing the site. It's not about
31 See in more detail the EDPB Guidelines 5/2020 on consent.
32 See also in more detail Decision 12/2019 of the Litigation Chamber.
33 CJEU judgment of 1 October 2019, C-673/17, Planet49, ECLI:EU:C:2019:801.

consent previously requested. However, it follows from Article 6.1 of the GDPR that this
Consent must be obtained prior to processing. By not getting
prior consent of the persons concerned, the defendant acted in violation of the

articles 6.1 a) and 7.1 of the GDPR.

142. In its response submissions of October 1, 2020, the Respondent acknowledged that the Policy regarding cookies could be improved. During the hearing, the defendant makes it known that in the meantime, the cookie policy has been brought into line with the legislation in force in terms of privacy and that henceforth, cookies are only placed when active consent has been obtained to this effect. The Inspection Service observes also that the defendant does not comply with article 7.3 of the GDPR in which it is stated that the data subject should have the right to withdraw consent at any time.
In the first version of the cookie policy reviewed by the Service of Inspection on July 13, 2020, the latter notes that no information is given to the data subjects on their right to withdraw the consent they give for the use of cookies. The statement relating to cookies that was used was as follows34:
"By using this site or by clicking "Approve", you consent to the use of cookies". An option saying "OK, I agree" was also displayed. Apart from the consent button, no other option was offered nor the possibility to withdraw the consent given.
143. In its submissions in response, with regard to the possibility of withdrawal from the consent for cookies, the defendant declares the following35:
"Finally, the Inspection Service states that the persons concerned are not sufficiently informed about their right to withdraw their consent for the use of cookies.
This is incorrect. First, the privacy statement generally states that
"For certain processing operations, you have the right, as a data subject, to withdraw your consent free of charge at any time". This right can of course also be exercised when consent has been given for cookies. Additionally, the statement of privacy specifically mentions for cookies how these cookies can be deleted by users: "Your browser settings allow you to to prevent the use of cookies or to receive certain notifications during installation

or the deletion of cookies. [...]”

By clicking on the links of the aforementioned browsers, a detailed explanation is provided

on how to delete cookies (the link to Google Chrome shows e.g. well in

34 Screenshot of the website taken by the Inspection Service.

35 Respondent's Response, p. 19.

highlight "Allow or block cookies"). In practice, the user can therefore decide

at any time that cookies can no longer be processed."

144. The Litigation Division does not share the defendant's position and agrees in this regard with

the finding of the Inspection Department according to

which in

the first version

(of July 13, 2020) of the cookie policy, the defendant has not complied with the

requirements of Article 7.3 of the GDPR, worded as follows: "The data subject has the right to

withdraw consent at any time. The withdrawal of consent does not compromise the

lawfulness of processing based on consent given prior to such withdrawal. The person

concerned is informed before giving consent. It is also easy to remove

than to give consent."36 According to the Litigation Chamber, it is clear that

withdrawing consent is not as simple as giving it. In addition to the button allowing

to accept the cookie policy, no choice was offered to withdraw the

consent given. As described in point 8, the data subject had to go through

several steps through browser settings before consent can be

took of. The Litigation Chamber therefore finds a violation of Article 7.3 of the GDPR.

145. On December 6, 2020,

the Litigation Chamber has analyzed

the site

Internet

https://www.westtoer.be in order to check whether changes had been made in the

respondent's cookie policy since the Inspection Service investigation,

as indicated above. It was indeed the case. The Litigation Chamber finds

that in the window for managing cookies, a distinction is now made between

the following cookies: essential, functional, analytical, advertising. The "essential" cookie

is pre-checked and it is not possible to uncheck it. Other - non-essential - cookies

can be checked but they are normally unchecked.

146. The cookie policy, in its current form, does allow individuals to

concerned to withdraw their consent as easily as giving it. Indeed, the

window for managing cookies mentions the following: “Do you want to take advantage of a

optimal experience? Click below on "Accept" if you agree to the use of

cookies for all the aforementioned purposes". You can also set your own

preferences. You can adapt your choices again at any time." Next to the button

"Accept", there is a button "adapt preferences" through which a consent

given can easily be withdrawn.

36 Emphasis by the Litigation Chamber.

147. The Litigation Division takes note of the foregoing. Given the fact that the policy on

of cookies has been adapted in the meantime, the Litigation Chamber limits itself to inflicting a

reprimand for violations of Article 6.1 a) and Articles 7.1 and 7.3 of the GDPR found

by the Inspection Service.

2.4.2. Register of processing activities (Article 30 of the GDPR)

148. Under section 30.1. of the GDPR, the data controller - and where applicable his

representative - must keep a record of the processing activities carried out under his

responsibility.

The Inspection Service has come to the conclusion that the defendant does not comply with article

30.1. According to the Inspection Service: the contact details of the controller are

incomplete and therefore not in conformity with article 30.1 a) (this because the e-mail address

dataverwerking@westtoer.be is not mentioned); the description of the categories of

persons concerned is not complete (article 30.1 c)), because in the column "categories of

natural persons", the word "other" is mentioned in several places; third countries

to whom the personal data are transmitted are not specified (article

30.1 e)) and there are several mentions of "(email addresses to Mailchimp)" without our knowledge

clearly which countries it is; the register does not mention data processing anywhere

personal data of visitors to the website through the use of cookies.

149. Respondent asserts in its pleadings that Westtoer's contact details cannot be

be qualified as incomplete only because of the absence of the e-mail address

dataverwerking@westtoer.be. According to the respondent, Article 30.1(a) of the GDPR does not require that

each e-mail address of the controller is mentioned. The register includes

indeed the contact details of both Westtoer and the Data Protection Officer. the

Respondent considers that Article 30.1(a) is thus complied with. The defendant also believes

incorrect to consider the description of the categories of data subjects as being

incomplete due to the use of the word "other". The defendant thus states that:

"a drop-down menu allows you to choose the following categories: (i) employees, (ii) customers, (iii)

suppliers, (iv) others, (v) applicants, (vi) website visitors. The "other" category

therefore targets data subjects who are not employees, customers,

suppliers, applicants or visitors to the website - such as, for example,

passers-by in the passers-by counting system. Taking into account the Service's remarks

of Inspection, Westtoer will adapt the register in order to designate the category "Others" with

more precision".

150. The Litigation Chamber took note of the register of processing activities and

notes that the contact details of both the controller and the data protection officer

data protection (as also indicated by the defendant) are included.

The e-mail address dateverwerking@westtoer.be does not appear among these

Data from the controller. However, the contact details of the person responsible for the

processing as well as the data protection officer are included in the register.

The Litigation Division considers that for the sake of completeness and good accessibility, it

it is recommended that you also include the above-mentioned e-mail address in the register.

The finding of the Inspection Service that the description of the categories of

data subjects is incomplete because the use of the word "other" is correct

in the facts. However, as the respondent explained in his pleadings, the register

includes different categories of which the "other" category is part and which is mentioned in

many times. A click on "details of the processing activity" of the register of the activities of

treatment determines which category is covered by "other". Bedroom

Litigation considers that on this point of the categories (article 30.1 c)), the register is not

contrary to the GDPR, but recommends that the defendant henceforth also explain the

"other" category.

151. The Litigation Division notes that the description of the third countries to which the data

personal character are transmitted lack of clarity. In the register of activities of

processing, under the tab transfer of personal data to third countries, it is

mentioned "yes (email addresses to Mailchimp)" with an additional link next to it.

By clicking on the link indicated, we arrive on Mailchimp's privacy policy which

indicates in which country this organization is established. In his pleadings, the defendant has

reported that resuming the link to Mailchimp's privacy policy indicates

that transfers of personal data may take place to the United States.

The Litigation Chamber considers it important to indicate henceforth explicitly and in a

unambiguous in the register of processing activities to which countries the personal data□

staff are transferred.□

152. In view of the foregoing, the Litigation Chamber considers that the register of the activities of□

processing does not comply on this point, which makes it possible to establish a violation of□

GDPR Article 30. This violation is not such as to require a sanction.□

2.4.3. The Data Protection Officer (Articles 37 and 38 of the GDPR)□

153. In accordance with Article 37.5 of the GDPR, the Data Protection Officer is appointed□

on the basis of his professional qualities and, in particular, his knowledge□

specialists in data protection law and practice. In the opinion of the□

Litigation Chamber, the documents that the defendant sent to the Service□

of Inspection sufficiently certify that the level of training and experience□

practice of the Data Protection Officer meet the requirement set out in Article□

aforementioned37. The defendant also complies with Article 37.7 of the GDPR since the data□

personal data of the data protection officer have been communicated by the□

defendant to the Data Protection Authority.□

154. Article 38.2 of the GDPR provides that the controller assists the delegate in the□

data protection in its missions by providing it with access to personal data□

personnel and by providing them with the necessary resources to carry out these missions.□

According to the Inspection Service, a violation of Article 38.2 of the GDPR is established since it does not□

It is not apparent from the Respondent's responses to how many agencies the Data Protection Officer□

data issues an opinion and what these agencies are. The defendant reacts as follows to the□

observation of the Inspection Service: "We do not know what the Inspection Service□

exactly blames Westtoer, but it seems that the Inspection Service claims that□

the agent would not have enough time to perform his duties as he only works in a□

4/5" speed.□

155. Respondent denies that the Data Protection Officer would not have sufficient
time, taking into account in particular the opinion issued in the file which is the subject of this
procedure. The Litigation Chamber notes that the GDPR does not require that a data protection officer
data protection officer is full-time.38 The delegate's opinion is also drafted in
detailed way. The Litigation Chamber considers that the documents presented do not allow
not to infer that there is a violation of Article 38.2 of the GDPR.
156. According to Article 38.3 of the GDPR, the delegate cannot receive instructions regarding
relates to the performance of his duties and he reports directly to the highest level of
the management of the controller. In response to questions from the Inspection Service,
the defendant communicated the following: "Within Westtoer, an employee has been appointed
to act as a contact person for the delegate. The delegate is associated with
ad hoc way - by phone or e-mail - via this implementation contact person
of the GDPR within Westtoer and gives notice to this contact person in accordance with
Article 38, paragraph 3". Group 29 has already stressed the importance of being able to report
to the most senior official in these terms: "Such direct reporting ensures that
senior management (e.g. the board of directors) is aware of the opinions and
37 Appendices 11 and 12 by e-mail from the defendant to the Inspection Service of August 18, 2020.
38 See also Group 29, Guidelines for Data Protection Officers (DPOs), WP 243 rev.01.

recommendations of the [data protection officer] which fall within the framework of
the mission of the latter consisting in informing and advising the data controller or
subcontractor". According to the respondent's response, the delegate gives notice to a person of
contact within the respondent's organization. According to the Litigation Chamber, the violation
of Article 38.3 of the GDPR is thus established. No violation was found to Article 38.6,
given that the data protection officer does not exercise other tasks and powers
for the defendant.

Publication of the decision

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

Litigation, in accordance with Article 95, § 1, 8° of the LCA, this decision is published

on the website of the Data Protection Authority, mentioning the data

of identification of the defendant39, and this because of the specificity of this decision - this

which makes re-identification inevitable, even in the event of deletion of the data

of identification - as well as the public interest of this decision.

FOR THESE REASONS,

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

-

that the smart camera system deployed by the defendant does not include any

breach of Article 5.1 a), b) and c) and complies with Article 25 of the GDPR;

-

to order the defendant, in accordance with Article 58.2, d) of the GDPR and Article 100,

§ 1, 9° of the LCA to put the information he provides about his processing

in its privacy statement in accordance with Articles 12 and 13 of the GDPR,

in particular with regard to the additional information that is requested

to the data subject in the context of a request on the basis of Articles 15 to 21

GDPR (Art. 12.6 GDPR), the legal bases for processing (Art. 13.1 c)

of the GDPR) as well as the retention periods for personal data

collected (art. 13.2 a) of the GDPR), and this within a period of one month from the

notification of this decision and to inform the Litigation Division thereof within the

same deadline;

-

pursuant to Article 58.2, d) of the GDPR and Article 100, § 1, 9° of the LCA, to order

the respondent to bring its record of processing activities into compliance with the

requirements of Article 30 of the GDPR and in particular to specify the third countries to which

39 Omitting, however, the name of the defendant's data protection officer.

data transfers are made within one month of the notification

of this decision and to inform the Litigation Chamber within the same period;

and

-

pursuant to Article 100, § 1, 5° of the LCA, to issue a reprimand vis-à-vis the

defendant following the violation of articles 6.1 a), 7.1, 7.3 (consent cookies) and 38.3

of the GDPR (direct report to the highest level of management of the person responsible for the

processing).

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

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

given as defendant.

(Sr.) Hielke Hijmans

President of the Litigation Chamber