1/35

Litigation room

Decision on the substance 15/2023 of 21 February 2023

File number : DOS-2021-03522

Subject: Complaint about the use of a geolocation system

The Disputes Chamber of the Data Protection Authority, composed of Mr Hielke

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

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

on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data and revocation of

Directive 95/46/EC (General Data Protection Regulation), hereinafter GDPR;

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

hereafter WOG;

Considering the regulations of

internal order, as approved by the Chamber of

Representatives on 20 December 2018 and published in the Belgian Official Gazette on

January 15, 2019;

Having regard to the documents in the file;

Made the following decision regarding:

The complainant:

X, hereinafter “the complainant”;

The defendant:

Y, hereinafter “the defendant”.

I. Facts and Procedure

Decision on the substance 15/2023/2023 - 2/35

1. On March 31, 2021, the complainant submits a complaint to the Data Protection Authority against

defendant.

The complainant was an employee of the defendant and, in that capacity, the main manager of a service car. In this context, he received a personal note containing registered injection times were compared with the vehicle's trip reports. The note stated that he has both his private address, if that of his mother, visited a certain café and some random streets which would constitute fraud. The complainant claims that he was not informed of the geolocation system (GPS tracking) in the service vehicles until he received the invoice. This According to the complainant, the geolocation system is also not mentioned in the work regulations. The the complainant subsequently submitted a request for the dismissal of this personal note to the mayor, but this was rejected. Consequently, the complainant has lodged this complaint.

2. On September 30, 2021, the complaint will be declared admissible by the First Line Service on pursuant to Articles 58 and 60 WOG and the complaint is dismissed pursuant to Article 62, § 1 WOG submitted to the Disputes Chamber.

3. On 27 October 2021, in accordance with Article 96, § 1 WOG, the request of the Disputes Chamber to carry out an investigation transferred to the Inspectorate, together with the complaint and the inventory of the documents.

4. On January 10, 2022, the investigation by the Inspectorate will be completed, according to the report appended to the file and the file is transferred by the Inspector General to the Chairman of the Litigation Chamber (Article 91, § 1 and § 2 WOG).

The report contains findings with regard to the subject of the complaint and states the following violations:

a.

infringement of Article 5(1)(a) and (2) and Article 6(1) of the GDPR; and

b.

violation of Article 5, Article 24(1) and Article 25(1) and (2) of the GDPR.

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

In general terms, the Inspectorate establishes the following infringements:

a.

infringement of Article 4, 11), Article 5(1)(a) and (2) Article 6(1)(a) and Article 7(1) and (2)

3 of the AVG for the use of cookies that are not strictly necessary;

b.

infringement of Article 12(1) and (6), Article 13(1) and (2) and Article 14(1) and (1), Article

5 (2), Article 24 (1) and Article 25 (1) of the GDPR;

c.

infringement of Article 30(1),(3) and (4) of the GDPR; and

d.

violation of Article 38(1) and (3) and Article 39 of the GDPR.

Decision on the substance 15/2023/2023 - 3/35

5. On February 4, 2022, the Litigation Chamber will decide on the basis of Article 95, § 1, 1° and Article 98

WOG that the file is ready for treatment on the merits.

6. On 4 February 2022, the parties concerned will be notified by registered mail

of the provisions as stated in Article 95, § 2, as well as those in Article 98 WOG.

They are also informed of the terms for their

to file defenses.

As regards the findings relating to the subject matter of the complaint, the

deadline for receipt of the statement of defense from the defendant

on 18 March 2022, those for the complainant's reply on 8 April 2022 and at

finally these for the statement of defense of the defendant on 29 April 2022.

As regards the findings that go beyond the subject of the complaint, the

deadline for receipt of the statement of defense from the defendant

on March 18, 2022.

7. On February 4, 2022, the complainant electronically accepts all communication regarding the case.

8. On February 7, 2022, the defendant electronically accepts all communications regarding the case.

9. On March 18, 2022, the Disputes Chamber will receive the statement of defense from the defendant with regard to the findings with regard to the object of the complaint. This statement also contains the response of the defendant regarding the findings made by the Inspectorate outside the scope of the complaint. In his conclusions, the defendant disputes the findings regarding the unlawfulness of the geolocation system does not. The defendant argues that since then she has a new geolocation policy has been drawn up and approved. This will be communicated to all employees involved. With regard to the third and fourth findings, the defendant to have worked out a new privacy statement and cookie policy. This new proposals are available for review by the ICT and Communication services of the defendant with the target date set for March 18, 2022. With regard to the fifth determination, the defendant agrees that there is ambiguity about the contact details of the DPO. This is clarified in the conclusions. Finally, the the defendant that it is the intention that the annual report will be made available for information on the agenda of the Board of Mayor and Aldermen and the Permanent Bureau after the has been presented to the Joint Management Team. Furthermore, the officer presents data protection issues formal advice to the City Council and the Council if necessary for Social Welfare and/or to the Board of Mayor and Aldermen / the Fixed desk.

10. The Disputes Chamber does not receive a statement of reply from the complainant with regard to the findings regarding the subject of the complaint. Then the Litigation Chamber also no conclusions of the defendant's rejoinder with regard to the findings regarding the subject of the complaint.

11. On September 28, 2022, the parties will be notified that the hearing will

take place on November 18, 2022.

12. On November 18, 2022, the party appearing will be heard by the Disputes Chamber. During the day

the hearing explains to the defendant what steps he has already taken in terms of

data protection since the submission of the complaint and the Inspectorate investigation.

13. On November 21, 2022, the minutes of the hearing will be sent to the party appearing

transferred.

14. The Disputes Chamber has no comments on behalf of the defendant

receive the report.

II. Motivation

15. The Disputes Chamber then assesses each of the findings included in the report

of the Inspectorate in light of the arguments put forward by the defendant in this regard

resources.

II.1. Article 5 (1) (a) and (2) GDPR and Article 6 (1) GDPR

II.1.1. Article 5 (1) a) and Article 6 (1) GDPR with regard to legality

16. The Litigation Chamber recalls that pursuant to Article 5(1)(a) GDPR personal data

must be processed lawfully, fairly and transparently. This means that the

processing must be based on the grounds for processing as set out in Article 6,

paragraph 1 GDPR. When personal data is processed lawfully, the

processing it properly. Finally, it must be clear for which

purposes personal data are processed and how this is done.

17. In further elaboration of this basic principle, Article 6 (1) GDPR states that personal data

may only be processed on the basis of one of the following legal grounds:

“a) the data subject has given consent to the processing of his

personal data for one or more specific purposes;

b) the processing is necessary for the performance of an agreement in which

the data subject is a party, or at the request of the data subject before the conclusion of

an agreement to take measures;

Decision on the substance 15/2023/2023 - 5/35

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

rests on the controller;

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

to protect another natural person;

e) the processing is necessary for the performance of a general task

interest or of a task in the exercise of public authority

has been assigned to the controller;

f) the processing is necessary for the protection of the justified person

interests of the controller or of a third party, except when

the interests or fundamental rights and freedoms of the data subject

that require the protection of personal data outweigh those

interests, in particular when the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing by public authorities

in the exercise of their duties."

Findings from the Inspection Report

18. The Inspectorate argues that the defendant has fulfilled the obligations imposed by Article 5(1)(a)

and paragraph 2 of the GDPR and by Article 6 of the GDPR. To this end, the

Inspectorate the following considerations apply:

a. "The program processes the number plate of the vehicle and

tracked, as well as the route followed. In principle, no names are given

directors, but a head of department knows in most cases

who is on the road with a vehicle." It is clear from the complaint that the defendant

concretely processed personal data of the complainant for the preparation and

delivery of a note dated October 14, 2020.

b. The defendant does not clarify in its answer on what legal basis

the personal data of the directors are processed, despite the

express request in this regard from the Inspectorate.

Defendant's position

19. In its submissions, the defendant disputes these findings of unlawfulness

processing of personal data in the context of the geolocation system is not. He poses

take the necessary steps to avoid this in the future and until then the geolocation system

no longer usable.

20. During the hearing dd. November 18, 2022, the defendant explains the steps taken

since the submission of the above claims. Meanwhile, on September 21

2021 approved a revised and up-to-date geolocation policy, in which the legal basis and

Decision on the substance 15/2023/2023 - 6/35

purposes for the data processing at issue were included. As for the

legal basis of the geolocation system, the defendant relies on it

legitimate interest (Article 6(1)(f) GDPR) in being able to trace its service vehicles.

The defendant states that he has made an extensive weighing of interests between

on the one hand its interest in operationalizing and optimizing its services, and on the other hand

the interest of employees not to be subjected to excessive

processing of their personal data.

Review by the Litigation Chamber

21. The Disputes Chamber points out that the complaint relates to the control of the work and

testing times in August and September 2020, but that the geolocation policy has been in place since

2009 until it was put on hold pursuant to the present proceedings.

22. The Disputes Chamber determines from the documents submitted by the defendant

that the processing of personal data collected through geolocation, by the defendant

started in 2009. On August 20, 2009, this geolocation system was discussed
during the meeting of the Special Negotiating Committee. In this context, it was
drafted an information document on the geolocation system on 19 August 2009.
A note on the modalities of the geolocation system and a step-by-step plan of the
its implementation was also drafted on August 19, 2009. After a collegiate
decision of the Board of Mayor and Aldermen was made on September 28, 2009
internal service note transferred to the staff, after which the geolocation system is switched on
came into effect.
23. It is important to note that the information document predates the
entry into force of the GDPR. Thus, no account could be taken of its creation
be taken into account with the obligations under the GDPR, but with the obligations
arising from Directive 95/46/EC, the legal predecessor of the GDPR.
In the
information document therefore becomes the
installation and use of it
geolocation system tested against the principles of purpose limitation, proportionality and
transparency. The Disputes Chamber concludes from this that the defendant has made a decision
has made to protect the right to privacy of the data subjects as much as possible
to protect. Also on September 28, 2009, an internal service note was distributed
within the Implementation service in which the geolocation system is explained. In this note
the various purposes are described, including combating unauthorized
use of service vehicles as well as mapping the movements so that the
proper and correct performance of the agreed work can be checked. The
note explains which data can be obtained by the geolocation system
(location of the car in real time, route traveled per day and per vehicle, etc.). In the note
it is also stated that only the heads of department

have access

till the

Decision on the substance 15/2023/2023 - 7/35

geolocation data via a license and login code. All the above information,

including examples of reports and a step-by-step implementation plan

transferred to the staff.

24. The GDPR has been applicable since 25 May 2018. The processing of personal data via

the geolocation system should thus be based on a basis as determined in

Article 6, paragraph 1 GDPR and the processing had to be done in accordance with the

principles from Article 5, paragraph 1 GDPR.1 It belongs to the controller

to indicate a lawful ground for its processing.2 This requirement also makes

part of the principles of legality and transparency that he must apply

(Article 5(1)(a) of the GDPR - as explained in Recital 39 of the GDPR).

Since different consequences follow from one or the other legal basis, with

in particular as regards the rights of the data subjects, it should be clear to the data subjects

on which legal basis the disputed processing is based. Serving those involved

therefore be informed of the legal basis of the processing in accordance with the

Articles 13 (1) (c) and 14 (1) (c) of the GDPR. As determined by the Inspectorate

the aforementioned 2009 information document does not state on what legal basis the

personal data of the directors are processed after they have been sent via the

geolocation system are collected, despite the express requests of the

inspection service in this regard. The defendant does not dispute this finding in its submissions.

25. In view of the above, namely the lack of identification of the appropriate

lawful basis for collecting and processing geolocation data

of the complainant, the Litigation Chamber concludes that the defendant has committed an infringement

to Articles 5(1)(a) and 6 GDPR as regards the period from 25 May 2018

to cessation of the processing operations in question following the findings of the

Inspection Service. In the present case, the Disputes Chamber finds that the defendant has already

was aware of the need to adjust the geolocation policy even before the

complaint was filed in this case, as a result of which the defendant acted negligently.

The Disputes Chamber is of the opinion that this is part of the normal pattern of expectations

a citizen whose data is processed by the government, who at the same time also their

employer is that the obligations under the AVG and other legal provisions -

proactive - be complied with. After all, the starting point should be that the defendant, just

like any other data controller, everything

puts in the work

process personal data in a correct manner in accordance with the

applicable regulations and does not adopt a wait-and-see attitude and therefore does not merely follow

on the merits 38/2021 of March 23, 2022, para 43, available from the web page

1 See decision

https://www.dataprotectionauthority.be/professioneel/publicaties/besluiten.

2 See decision on the merits 47/2022 of 4 April 2022, para 113 and decision 48/2022 of 4 April 2022, para 125 and 219,

available via the webpage https://www.dataprotectionauthority.be/professioneel/publicaties/besluiten.

intervention of the Data Protection Authority takes action to make that adjustment

to be achieved.3 However, the Disputes Chamber also takes into account the fact that the

defendant, already took into account when drawing up its geolocation policy in 2009

taking into account the principles of finality, proportionality and the rights of the data subjects.

In addition

the 2009 geolocation policy transparently informs the

those involved in the installed geolocation system.

26. During the hearing, the defendant points out that the geolocation policy was adopted in 2021

altered. This new policy explicitly explains that the geolocation system

is based on the legal basis of the legitimate interest as understood in Article 6, paragraph

1, f) GDPR. Consequently, the Litigation Chamber must verify whether the legitimate interest ex

Article 6 (1) f) GDPR can serve as the legal basis for such processing by the

defendant.

27. The last sentence of Article 6 (1) f) GDPR stipulates that this legal basis of the

legitimate interest does not apply to the processing of personal data by

government authorities in the exercise of their duties. The question therefore arises whether

the defendant can rely on this legal basis for the geolocation system.

28. Since the defendant is a public authority, the above must be assessed

in light of the principle of conferral of administrative powers, it

principle of the specialty of legal persons and the

principle of legality, that the

determines the conditions under which the administration can interfere with the right to

protection of privacy, of which the right to protection

personal data is part.4 According to the principle of attribution of

administrative powers, which is enshrined in Article 105 of the Constitution and Article

78 of the Special Institutional Reform Act of August 8, 1980, the

administrative authorities have no powers other than those formally vested in them

granted by the Constitution and the laws and decrees that are thereunder

issued. Furthermore, the specialty principle of legal entities states that each

legal entity may only act to achieve the purpose or purposes

achieve for which it was established, provided that only a legislature

standard can entrust a legal entity with a public service mission. The Council of

State, in its opinion on the draft law "on the protection of

natural persons with regard to the processing of personal data".

that "the passing of data from one government agency to another is a form of

interference with the right to the protection of privacy of the

See

also

decision

3

https://www.dataprotectionauthority.be/professioneel/publicaties/besluiten.

4 The CBPL has already pointed this out in its advice on the preliminary draft law that has become the WVG. See CPP, Advice

No. 33/2018, p. 44

the webpage

available

December

141/2021

2021,

by

through

16

Decision on the substance 15/2023/2023 - 9/35

data subjects. Under Article 8 of the European Convention on Human Rights and

Article 22 of the Constitution, as interpreted in the settled case-law of the

Constitutional Court, such interference must in particular have a legal basis

are proportionate to the objective pursued and are sufficient

be clearly organized so that it is foreseeable for the citizen"5.

29. In short, a government agency may only process personal data if this is the case

processing is necessary for compliance with an obligation imposed by or pursuant to a

legal provision has been imposed on one of the controllers (Article 6 para

1, c) GDPR) or if this communication is necessary for the performance of a task of
public interest assigned to one of the controllers by or
pursuant to a law (Article 6(1)(e) GDPR). The Disputes Chamber will determine as much as necessary
points out that it cannot be ruled out that in limited cases a public authority may appeal
do on Article 6(1)(f) but that this for the geolocation system as described by
the defendant is not possible. The legal basis from Article 6(1)(f) GDPR (legitimate
interest) cannot apply to the processing at issue.

30. In order for a controller to be able to rely on Article 6(1)(e) of the GDPR,
professions to process personal data, this processing must be necessary for
the fulfillment of a task of general interest or of a task within the framework of the
exercise of public authority vested in the controller
is
assigned.

31. The Disputes Chamber notes that the AVG offers no starting point for the
answering the question to what extent understanding "processing necessary for the
performance of a task in the public interest" would also include human resources management.

32. However, a clear starting point for a broad interpretation of this concept is possible
found in Regulation (EU) No. 2018/1725 of the European Parliament and the
Council of 23 October 2018 on the protection of natural persons in relation
with the processing of personal data by the institutions, bodies, offices and agencies of the
Union and the free movement of such data, and repealing Regulation (EC) No.
45/2001 and Decision no. 1247/2002/EC, recital 22 of which reads: "[...]. The processing of
personal data for the performance of the tasks assigned by the institutions or bodies of
the Union in the public interest includes the processing of the
management and operation of those institutions and bodies [...]".

33. From this consideration, the Litigation Chamber deduces that Article 6(e) GDPR is not alone

relates to processing operations that are necessary for the fulfillment of

5 Opinion of the Council of State no. 63.192/2 of 19 April 2018, in Parl. St., K., Regular Session, 2017-2018, no. 54-3126/001,

p.

421-422

the task of public interest in the strict sense, but also to processing that is necessary

for the performance of duties directly related to that duty of general

interest, including those necessary for the management and operation of the

bodies entrusted with that task of general interest.

34. The Knowledge Center of the GBA has already confirmed that the processing of

personal data by a government in the context of the management of its personnel

means can take place on the basis of 6 (1) e) GDPR provided that the taken

measures are actually necessary.6

35. In view of the above, the Litigation Chamber concludes that the concept of "processing that

necessary for the performance of a task carried out in the public interest".

to be interpreted. Consequently, the notion of "processing necessary for the

performance of a task of public interest" refers to processing that is necessary

are for the fulfillment of the task of general interest in the strict sense, but also on

processing that is necessary for the performance of tasks that are directly related

with that task of public interest, including those necessary for

the management and functioning of the bodies entrusted with that task of general interest.

Since the defendant without personnel and associated management of human resources

could not perform its tasks in the public interest, processing of

personal data in the context of personnel management should also be based on

Article 6 (1) e) GDPR. 7

36. In order to legitimately rely on the legal basis of Article 6(1)(e) GDPR

personal data may therefore only be processed if this is necessary for the

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

of the public authority entrusted to the controller. The processing must

in these cases always have a basis in the law of the European Union or that of the

Member State concerned, which must also state the purpose of the processing. Consequently, there must be

whether these conditions are met in this case.

37. Pursuant to Article 6(3) and Recital 45 of the GDPR, processing based on

Article 6(1)(e) GDPR meet the following conditions:

a. The controller must be responsible for fulfilling a

assignment of public interest or an assignment that forms part of the

exercise of public authority on any legal basis, regardless

6 See, among others, GBA, recommendation 02/2020 of 31 January 2020 regarding the scope of the obligation to draw up a

protocol

close to the communications of personal data by the

formalize

https://www.dataprotectionauthority.be/publications/aanbeveling-nr.-02-2020.pdf.

7 GBA, Recommendation 02/2020 of 31 January 2020 on The scope of the obligation to conclude a protocol

for the announcements

formalize

https://www.dataprotectionauthority.be/publications/aanbeveling-nr.-02-2020.pdf.

of personal data by the

federal public sector the

federal public

sector de

whether it is in the law of the European Union or in the law of the Member States

contained;

b. The purposes of the processing are determined or must be stated in the legal basis

are necessary for the performance of the public interest assignment or the

exercise of public authority.

38. The Litigation Chamber will determine the conditions of public interest, legal basis and

assess necessity below.

Public interest task

39. In this case, the defendant adopted the geolocation policy in order, on the one hand, to

professional use of the service vehicles and the proper execution of it

to check assigned work within the planned work schedule and, on the other hand, to check the

monitor staff in the performance of their duties. The Disputes Chamber is therefore of

believes that the public interest lies in scarce government resources, in this case the

deploy fleet and personnel efficiently and to prevent fraud and misuse of services

so that these resources can be used for the performance of the tasks

assigned to the congregation.8

A clear, precise and predictable legal basis

40. According to recital 41 of the GDPR, this legal basis or legislative measure

be clear and precise and its application must be for the litigants

be foreseeable, in accordance with the jurisprudence of the Court of Justice of the

European Union (hereinafter: Court of Justice) and the ECHR. The European Court of Rights of

de Mens (hereinafter: ECtHR) used the concept of predictability in the Rotaru judgment9

legal basis specified. Since that case involved surveillance systems

of a state's security apparatus, the context of the present case differs. In

in other cases, the ECtHR has indicated that it adheres to these principles

can be guided, but it considers that these criteria, which in the specific context of

that specific case have been established and followed thus not as such on all cases of

apply10.

41.

Pursuant to article 186, §1 of the Local Government Decree11, the municipal council of each

municipality determines the legal status of municipal employees. The city council and

the council for social welfare establish a joint deontological code

for the staff. This concretises the provisions included in the Local Decree

8 See by analogy recital 47 of the GDPR.

9 ECtHR, 4 May 2000, Rotaru v. Romania.

10 ECtHR, 2 September 2010, Uzun v. Germany, § 66.

11 Decree on Local Government of 22 December 2017, Belgian Official Gazette 15 February 2018.

Board and can assume additional deontological rights and obligations,

in accordance with the organizational management system, as stipulated in articles 217 and

220 of the Local Government Decree12 The organizational system to be

adopted by each municipality is described as the set of measures and

procedures designed to provide reasonable assurance that one:

1° achieves the set objectives and knows and manages the risks involved in achieving them;

2° comply with legislation and procedures;

3° has reliable financial and management reporting;

4° works in an effective and efficient manner and the available resources are economical

stake;

5° protects the assets and prevents fraud.13

42. In view of the above, the defendant is under a statutory obligation to take measures

and establish procedures with regard to its organization to ensure that they are on

works efficiently with an economic use of resources and prevents fraud,

without explicitly specifying how this should be done concretely.

43. The Litigation Chamber has already pointed this out in decision 149/2022 dd. 18

October 202214 that tasks of public interest or public authority with which

controllers are in charge, often not based on accuracy

defined obligations or legislative standards, which define the essential features of the

capture data processing. Rather, processing takes place on the basis of a

more general authorization to act, such as for the fulfillment of the task that

necessary, as is the case here. This leads to the relevant legal

basis in practice often does not contain any concretely defined provisions regarding the

necessary data processing. Controllers who are based on

want to invoke such a legal basis on Article 6 (1 e) GDPR, you must do so yourself

verify whether the processing is necessary for the task of public interest and interests

of those involved.

Necessity

44.

Pursuant to Article 6(1)(e) GDPR, processing is lawful only if and for

insofar as the processing is necessary for the performance of a task carried out in the public interest or

of a task in the context of the exercise of public authority vested in the

controller

is assigned. Contains as explained above

12 Article 193, §1, second paragraph Decree on Local Government.

13 Article 217 Decree on Local Government.

14 See also decision 124/2021 dd. November 10, 2021.

legislation often lacks concretely defined provisions regarding the necessary

data processing.

45. The Court of Justice ruled on this condition of

necessity:

“Given the aim of providing equivalent protection in all Member States, the concept

necessity as it emerges from Article 7(e) of Directive 95/46, which a

want to provide precise delineation for one of the cases in which the processing of

personal data is permitted, i.e. does not have a content that differs from Member State to Member State

member state. It is therefore an autonomous concept of Community law, which it must

be interpreted in a way that fully fulfills the purpose of the directive such as

defined in Article 1(1).'16

46. The Advocate General has also argued

in his conclusions that

"[It

concept of necessity [has] a long history in Community law and a

an integral part of the proportionality criterion. It means that the authority that

to achieve one

legitimate purpose establishes a measure that a

Community law affects guaranteed rights, must demonstrate that this measure is the

least restrictive to achieving this goal. In addition, when the processing of

personal data can lead to an infringement of the fundamental right to respect for the

privacy, Article 8 of the

European Convention for the Protection of Human and Fundamental Rights

freedoms (ECHR), which guarantees the right to respect for private and family life.

As the Court stated in Österreichischer Rundfunk and Others, a national

regulation that is not in accordance with Article 8 of the ECHR, also do not comply with the provisions of Article 7, sub e, of

requirement laid down in Directive 95/46. Article 8(2) of the ECHR provides that interference with the

private life is permitted to the extent that it serves one of the purposes listed herein

is pursued and it is 'necessary in a democratic society'. According to it

European Court of Human Rights keeps the adjective 'necessary'

in that a "compelling social need" for a particular action by the

government exists and that the measure is proportionate to the legitimate aim pursued.

47. This case law formulated in relation to Article 7(e) of Directive 95/46/EC

remains relevant to this day. Article 6(1) of the GDPR takes over the wording from

Article 7 of Directive 95/46/EC.

15 CJEU, Heinz Huber v. Bundesrepublik Deutschland, December 16, 2008, C-524/06.

16 CJEU, Heinz Huber v. Bundesrepublik Deutschland, December 16, 2008, C-524/06, para. 52.

48. The Court of Justice has also clarified that if there are realistic and less

are radical alternatives, the treatment is not "necessary".17

49. The Litigation Chamber therefore serves

to assess whether it

installing it

geolocation system was necessary for the aforementioned public interest and whether there

other less invasive options were to pursue the aforementioned public interest

to strive. The necessity of a geolocation system is evident from the fact that the report

of the meeting of the special negotiating committee of the defendant at which the

geolocation system was explained and discussed, mentions that the organization of the

fleet of the A should be better monitored as there were quite a few in the past

have been incidents that could not pass the bracket. Since these incidents

relate to movements outside the buildings or premises of the defendant,

states that it is impossible for him to verify in any other way whether the

fleet is used optimally and to detect and prevent possible fraud.

The geolocation system aims to put an end to these practices.

50. Recently, in the judgment in Florindo de Almeida Vasconcelos Gramaxo v. Portugal18

spoke out about the use of geolocation systems for professional

track movements. The ECtHR states that, by using only the geolocation data that

relate to the professional displacements, to handle, the interference on it

right to protection of private life was limited to what was necessary for the

defense of the public interest of the defendant. The Disputes Chamber states that it

processing of personal data via a geolocation system is therefore only possible

in the specific circumstances set out in this judgment. In the present case, the

findings of the ECtHR by analogy with

application. The processed

personal data also only relates to professional travel, with a

service car19, which is necessary for the promotion of the public interest, te

know how to prevent fraud and the proper management of public funds.

51. In view of the above, the geolocation system does indeed constitute an interference

the right to protection of the private life of those concerned, but this one is earlier

limited. The Litigation Chamber notes that if the processing of geolocation data

takes place under the conditions set20, namely with regard to professional

movements within working hours with a service car and limited to the data that

17 CJUE, Volker & Markus Schecke GbR and Hartmut Eifert t. Land Hessen, 9 November 2010, Joined Cases C□92/09

and C□93/09

18 ECtHR, 13 December 2022, Florindo de Almeida Vasconcelos Gramaxo v. Portugal, para 120-122.

19 In Florindo de Almeida Vasconcelos Gramaxo v. Portugal, it concerned a company car that could be used

for private and professional trips, but only the geolocation data of the professional

transfers could be processed by the employer.

20 In Florindo de Almeida Vasconcelos Gramaxo v. Portugal, it concerned a company car that could be used

for private and professional trips, but only the geolocation data of the professional

transfers could be processed by the employer.

are necessary, with the necessary guarantees that the processing of the data collected
is done in accordance with the basic principles of Article 5 (1) GDPR, which in addition
explained transparently, this system constitutes a less invasive interference than
other methods of surveillance. Moreover, for the defendant there is no other
feasible method to monitor the cars and the service movements in the context of
the above-mentioned goals. In addition, consultation will only be possible by a limited number
number of persons described in the geolocation policy and if there is a specific
there is reason to.

II.1.2. Article 5(1)(a) GDPR with regard to transparency

52. When the controller bases a processing on the public interest,
then he must be transparent about this because of, among other things, the public interest pursued
name, to make clear for what purposes the personal data are processed,
which personal data is processed, whether the data is shared with others
parties and how long the personal data is kept.

53. As already mentioned, the defendant has drawn up a new geolocation policy. During the day
the hearing provides the defendant with a draft of this amended
geolocation policy. In this, the defendant explains and explains the legal basis and purposes
he explains how the geolocation system works and how the people involved
prior to moving with a vehicle equipped with such a system
to verify its presence. In addition, the policy determines which data is there
and not processed and for what purposes this data is processed and for
which purposes it is not (such as checking speed limit compliance, a
monitor employee permanently, etc.). Next, the geolocation policy clarified
who has access to the personal data, how access can be obtained
by these persons (such as via a login code) and the retention period of the data. The

Defendant notes that the new geolocation policy has yet to be approved

– early 2023 – after which the geolocation system can be started up. In this context

the defendant will develop a process to explain this new policy to all

persons involved, for which a signature will be required for acknowledgment.

54. The Disputes Chamber is of the opinion that the mere fact that the defendant is not the correct one

lawful basis has applied in the past the processing in the future

not necessarily invalid. The Litigation Chamber notes that it is as above

described collection and processing of geolocation data may be lawful,

if the appropriate legal basis is correctly determined and the above

transparency obligations in this regard are complied with by the defendant

of its staff. The Disputes Chamber refers to the design of the new

geolocation policy approved by the City Council on September 21, 2021.

Since only the data related to the movements carried out in the context of

the performance of (certain aspects of) the job, is the degree of interference with the law

on data protection limited to what is necessary to protect the public interest

pursuit, namely the proper organization and management of public funds of the

defendant on the other. The Disputes Chamber therefore states that the processing of

personal data collected through a geolocation system can be done by the

defendant provided that the conditions of Article 6(1)(e) are met.

II.2. Article 5 of the GDPR, Article 24(1) of the GDPR and Article 25(1) and (2) of the

AVG

II.2.1. Article 5 (2) GDPR, Article 24 (1) and Article 25 (1).

55. The Litigation Chamber recalls that each controller has the

basic principles on the protection of personal data as understood in Article 5,

must comply with paragraph 1 GDPR and must be able to demonstrate this. That follows from the

accountability in Article 5(2) GDPR in conjunction with Article 24(1) GDPR as

confirmed by the Litigation Chamber21.

56. Based on Articles 24 and 25 of the GDPR, the defendant must take appropriate technical and

take organizational measures to ensure and be able to demonstrate that the

processing takes place in accordance with the GDPR. The defendant must do so

effectively implement data protection principles, the rights of data subjects

as well as only process personal data that is necessary for each

specific purpose of the processing.

57. As part of its investigation, the Inspectorate assessed to what extent the

the defendant has taken the necessary technical and organizational measures to

comply with these principles from Article 5 (1) GDPR and in particular the principle of

legality and transparency (see II.1). In this regard, the Inspectorate decides that the

the defendant has not sufficiently demonstrated that he has taken the necessary measures

for the processing at issue to take place in accordance with Article 5(1) a) and Article

6 (1) GDPR, since the Inspection Service has concluded that the processing

were inconsistent with these principles.

58. During the hearing, the defendant explained that

meanwhile a new one

geolocation policy has been drawn up and approved. This is the next step in the process

to communicate to all employees involved, according to the defendant. In this way

does the defendant want to comply with the guidelines on making the way of

work towards employees.

Decision

21

https://www.dataprotectionauthority.be/professioneel/publicaties/besluiten.

ground

2020

available

by

June

ten

23

34/2020

through

the webpage

Decision on the substance 15/2023/2023 - 17/35

59. The Litigation Chamber ruled in part II.1 that there was indeed an infringement

to Article 5(1)(a) GDPR with regard to legality for the period between 25 May

2018 and the time when the defendant ceased the disputed processing. For

with regard to the transparency principle, the Litigation Chamber notes that

in the

geolocation policy from 2009 and the accompanying internal memorandum show that the

employees have been informed, but the defendant does not show that they

in this respect complies with accountability since the entry into force of the GDPR,

for example by updating the geolocation policy

and request confirmation of receipt from the employees concerned. As

already explained above, the defendant had to check on its own initiative whether

he complies with the obligations under the GDPR from 25 May 2018. The Disputes Chamber therefore argues

established that the defendant could not demonstrate that he had the necessary technical and organizational

has taken measures to comply with the principle of legality and the

principle of transparency as understood in Article 5(1)(a) GDPR since 25 May 2018. Therefore

the Disputes Chamber rules that there is a violation of Article 5(2) in this context

Article 24 (1) and Article 25 (1) GDPR.

II.2.2. Article 5 (1) GDPR

60. Although Article 5(1) and (2) GDPR are closely linked, any one means

violation of the accountability obligation of Article 5 (2) GDPR is not automatically also a

Violation of Art. 5 (1) GDPR. After all, accountability is the formal one

externalization through documents to ensure compliance with the material

basic principles of the GDPR.

61. As regards compliance with Article 5(1)(a), the Litigation Chamber refers to section II.1

of this decision. As regards the basic principles contained in Article 5(1),

b) up to f) the Disputes Chamber has insufficient elements to make an assessment

to go over.

II.3. Article 4, 11) of the GDPR, Article 5, paragraph 1, a) and paragraph 2 of the GDPR, Article 6, paragraph 1, a) of the

GDPR and Article 7, paragraph 1 and paragraph 3 of the GDPR for the use of not strictly necessary

cookies

62. Based on Article 4, 11), Article 5(1)(a) and (2), Article 6(1)(a) and Article 7(1) and (3)

GDPR, it is necessary that the controller who invokes the consent

as a legal basis for the processing, can demonstrate that the data subject has effectively consented

has given. Article 7, paragraph 3 GDPR sets strict conditions for withdrawing a

valid permission.

II.3.1. Findings from the Inspection Report

63. The Inspectorate first established that there could be no question of a valid

consent to the placement of cookies that are not strictly necessary, given on the one hand the

interface design of the cookie banner and, on the other hand, the flawed information in it

cookie policy. Secondly, the Inspectorate finds that the defendant did not comply with

the conditions regarding the withdrawal of a valid consent.

64. With regard to the consent process and more specifically the

interface of the

cookie banner, the Inspection Service determines that a data subject on the cookie banner two

options for the use of cookies that are not strictly necessary, namely

on the one hand 'continue' and on the other hand 'more info'. These were not on an equal footing

way displayed. In addition, the choice was missing in the cookie banner that came with the

opening the website allows data subjects to use not strictly necessary

cookies in the first information layer by refusing one click.

65. With regard to the transparency obligations in the context of an informed

permission, the Inspectorate has determined that the defendant's data subjects

did not receive transparent information about the consequences for their personal data

the use of cookies. After all, the defendant was informed by the parties involved in the

cookie window is not given an explanation of the consequences of their choice. The privacy statement

of the defendant provided only vague information about the consequences for them

personal data through the use of cookies by the defendant, such as which are not strict

necessary cookies exactly the defendant uses on its website and what the purposes

of the processing of the personal data of the data subjects for each of them

cookies; how long the personal data of the data subjects that were processed via not

Strictly necessary cookies are stored on the defendant's website or which ones

the criteria are for determining that period; what concrete steps should be taken by those involved

if they wanted to change the cookie settings via their internet browser.

66. Finally, no explanation was given to data subjects in the cookie window about how a

given consent can be withdrawn.

67. In view of the above, the Inspectorate has determined that there are no legally valid

consent within the meaning of Article 5, Article 6 (1) a) and Article 4.11) in conjunction with Article 7 GDPR

asked the website visitors for the use of not strictly necessary

cookies, which means that it cannot be demonstrated either.

II.3.2. Defendant's position

68. First, the defendant emphasizes that the process of updating its cookie and cookie policy had already started, even before he was informed of the findings of the Inspection Service and shortly afterwards the new cookie and cookie policy implemented on the website and the permission policy regarding the use of

cookies on the website. The cookie banner has been adjusted so that the data subject is no longer steered in a certain direction with regard to the placement of analytical and other not strictly necessary cookies. The person concerned can also contact any visit the website in a simple way to adjust his preferences again via a link 'cookie settings' at the bottom of the website. By way of illustration, the defendant makes several screenshots about.

69. With regard to these findings, the defendant argues that a new cookie policy was worked out. At the time of drafting the conclusion, the proposal was with his services ICT and Communication for review and implementation was scheduled for March 18, 2022. During the hearing, the defendant explains that the new cookie policy is now transparent explains which cookies are used, for what purposes this happens, what what happens to the collected data, how the data subject can manage its use, when the defendant passes the cookies on to third parties and under which conditions this would happen. The defendant also points out that in the new cookie policy it is indicated how the data subject can determine via the browser settings how the web browser handles cookies. Furthermore the new cookie policy informs the data subject about his rights and about the possibility of contacting the defendant as controller, or with the officer for

data protection, and how the visitor can manage its use, when the

cookies are passed on to third parties and, if applicable, under what conditions.

Finally, the new cookie policy also informs users about their rights and the

possibility to contact the defendant as controller,

or with the data protection officer.

II.3.3. Review by the Litigation Chamber.

70. With regard to legal consent within the meaning of the aforementioned articles,

the Litigation Chamber determines that the interface of the cookie banner and the cookie policy

were indeed adjusted since the Inspection Report, as indicated by the

defendant at the hearing. Although the adjustments were only made after the

intervention of the Inspectorate, which does not detract from the earlier

findings of the Inspectorate, the Litigation Chamber will only discuss the new ones below

cookie banner and review the new cookie policy. by the Inspectorate

the established infringements were after all clear and were not contested by the defendant.

71. The Litigation Chamber will first assess the consent process, in particular the interface

of the cookie banner and the information obligations regarding the cookies in the cookie policy.

Subsequently, the Litigation Chamber will check whether the conditions regarding the withdrawal of the

valid permission was respected.

Decision on the substance 15/2023/2023 - 20/35

1. Consent lawfully given

72. Before examining whether there is valid consent in the present case,

reminds the Litigation Chamber of the conditions that must be met in order for a

legally valid consent. Article 5.3 of the ePrivacy Directive22,

as transposed in article 10/2 of the law of 30 July 2018 on the protection of

natural persons with regard to the processing of personal data (hereinafter:

Data Protection Act).23 stipulates that the consent of the data subjects is required

for placing the cookies, except when it comes to strictly necessary cookies.

73. Recital 17 of the ePrivacy Directive clarifies that for its application the concept “consent” should have the same meaning as “data subject's consent” such as defined and specified in the Data Protection Directive 95/46/EC (which is now replaced by the GDPR). This was also clarified in guidelines on consent by the Data Protection Group.24

74. Article 4, 11) GDPR defines “consent” of the data subject as “any free, specific, informed and unambiguous expression of will by the data subject by means of a statement or an unequivocal active act concerning him processing of accepts personal data”.

75. Article 7 GDPR stipulates the conditions applicable to the consent:

1. When processing is based on consent, the controller must be able to demonstrate that the data subject has given consent to the processing of his personal data.

2. If the data subject gives consent in the context of a written statement that also relates to other matters, the request for consent shall be submitted in an intelligible and easily accessible form and in clear and plain language presented in such a way that a clear distinction can be made from the others matters. When any part of such statement constitutes an infringement to this regulation, this section is not binding.

3. The data subject has the right to withdraw his consent at any time. Withdrawing leave the lawfulness of the processing based on the of the permission withdrawal thereof, without prejudice. Before being the data subject permission before the consents, he will be notified thereof. Withdrawal of consent

is as simple as giving it.

22 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002

23 Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, B.S., September 5, 2018.

24 EDPB, Guidelines 5/2020 on consent under Regulation 2016/679, 4 May 2020, i.a. para.7.

4. When assessing whether consent can be freely given, the take into account, among other things, the question whether for the implementation of a agreement, including a service agreement, requires consent a processing of personal data that is not necessary for the implementation of that agreement.

1.1 Consent lawfully given: cookie banner

76. With the new cookie banner, the visitor to the website is given the choice of, on the one hand, the manage or otherwise agree to cookie preferences (i.e. all not strictly accept necessary cookies = global opt-in button). When you click on the option 'Manage cookie preferences', more information appears about the cookies that are used are divided into the following three categories: “necessary”, “analytical cookies” and "cookies with your preferences" where information is always provided in understandable language the purpose of these cookies. The data subject can therefore, as far as the not strict necessary cookies, give the consent per above category. So there is none button present at the same level as the global opt-in button where the can refuse permission for all non-strictly necessary cookies. Referring to it report of the Task Force Cookie Banner of the European Data Protection Board (EDPB)25, the Disputes Chamber notes that these adjustments to the new cookie banner are already a step

are in the right direction with regard to the findings of the Inspectorate with

regarding the old cookie banner.

77. For the sake of completeness, the Disputes Chamber notes the following matters. First

the aforementioned Task Force Cookie Banner report clarifies the rules regarding a

legally given consent. There should be a button for rejecting all non-strict

necessary cookies to be available at the same level of information as the global opt-

on the first information layer26, for example by buttons with the title “accept all”

and “reject everything”. At the moment, the new cookie banner only provides an opt-in button

but no global button to deny permission. In view of the publication of this report

after closing the debates, the Litigation Chamber formulates the above as

recommendation.

78. Secondly, the Disputes Chamber also notes that in the new cookie banner the button “my

manage choice” is white, like the background of the cookie banner, while the button “all

accept cookies” has a turquoise background, which contrasts with the white one

background, and thus directs the data subject to accept all cookies. For as much as

25 EDPB, Report of

17

https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

26 EDPB, Report of

17

https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

the Cookie Banner Task Force,

the Cookie Banner Task Force,

the work undertaken by

the work undertaken by

January 2023,

necessary, the Litigation Chamber points out that the aforementioned report of the Cookie Banner Task Force from the EDPB states that this may constitute an invalid consent, but in this case must be assessed on a case-by-case basis.27 In view of the publication of this report after the close of the debates, the Litigation Chamber formulates the above as a recommendation.

1.2 Consent lawfully given: cookie policy

79. The Litigation Chamber notes that the cookie policy has been amended in accordance with the most of the Inspectorate's comments. The Disputes Chamber takes this deed and will now only discuss the new cookie policy. Although the new cookie policy even though it takes steps in the right direction compared to the old cookie policy that was examined by the Inspectorate, it is recommended that the following elements also to provide for the new cookie policy. First, the Disputes Chamber determines that the cookies present are divided into the following three categories: necessary, analytical and cookies with preferences. The Litigation Chamber finds that in the category 'cookies with your preferences' contains cookies with different purposes. So would the cookies with the purpose of collecting user feedback to improve our website improve, better placed in the category of analytical cookies, while the cookies for the purpose of “capturing your interests in order to provide tailored content and to be able to offer offers' have marketing as their purpose. Considering the principle of granularity, the Litigation Chamber formulates the recommendation to classify the cookies 'cookies with your preferences' can also be classified per objective. This allows the person concerned to make a more nuanced choice. Secondly, the Litigation Chamber notes that it is not clear from the cookie policy to whom the data collected via the cookies is being sent. The Litigation Chamber also recommends that these recipients also be registered to take

in the cookie policy. Finally, the Disputes Chamber points out that with the

browser settings no valid consent can be collected regarding the

AVG. On the one hand because the users cannot (yet) give permission according to

the purposes pursued by the different types of cookies. The permission given through the

browser settings is therefore not sufficiently specific with regard to the

requirements of the AVG.28 On the other hand, because the browser settings can be standard

provide for the acceptance of the cookies, without the data subject being aware of this

is, as a result of which the consent does not constitute an explicit active act and is therefore not

is legally valid within the meaning of the GDPR.

27 EDPB, Report of

https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf, p. 6 and 7.

28

the

consult

https://www.dataprotectionauthority.be/professioneel/thema-s/cookies.

the Cookie Banner Task Force,

the work undertaken by

Cookies

website

theme

GBA,

also

by

See

on

the

17

at

January 2023,

through

80. In view of the above, the Disputes Chamber rules that there was an infringement

to Article 4, 11), Article 5, paragraph 1, a) and Article 6, paragraph 1 GDPR, and that these have been partially remedied

Decision on the substance 15/2023/2023 - 23/35

became.

2. Withdrawal of a given consent

81. With regard to the transparent information about the withdrawal of a data

consent to the use of cookies that are not strictly necessary, remembers the

Litigation Chamber that the data subject has the right under Article 7(3) GDPR

has to withdraw his consent at any time, and that the withdrawal of the

consent should be as simple as giving it. The person concerned must do so

shall be notified of this right under the same provision, before he is

gives permission.

82. In this context, the Litigation Chamber notes that at the bottom of the website a link 'cookie

settings' is available, whereby the data subject returns to the above

selection menu from the cookie banner regarding the consent of the categories of cookies.

According to the aforementioned Cookie Banner Task force report, the website

provide readily available options to withdraw consent, at any time

moment, such as by placing a link in a visible and obvious place.29 The link

"cookie settings" is located at the bottom of the defendant's website, where common

the links to the privacy policy and cookie policy are there, and the link is at any time

accessible. The Disputes Chamber therefore concludes that the defendant is transparent

provides information and functionality about withdrawing a given consent

the use of cookies that are not strictly necessary in accordance with Article 7 (3) of the GDPR.

83. In view of the above, concludes that there is no longer any infringement of

Article 7 (3) GDPR. This does not alter the fact that there was a historic breach that has since been

remedied.

II.4. Article 12(1) and (6) GDPR, Article 13(1) and (2) GDPR and Article 14(2) GDPR

1 and paragraph 2 GDPR, Article 5 paragraph 2 GDPR, Article 24 paragraph 1 GDPR and Article

25 (1) GDPR

84. Based on Article 12(1) GDPR, Article 13(1) and (2) GDPR and Article 14(1)

and paragraph 2 of the GDPR, it is necessary for the defendant to be the controller

provides the data subjects with concise, transparent and comprehensible information about the

personal data being processed. The aforementioned transparency obligations

a concretization of the general transparency obligation of Article 5(1)(a) of the

AVG. As already explained, the defendant must have the appropriate technical and

29 EDPB, Report of

https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf, p. 8.

the Cookie Banner Task Force,

the work undertaken by

17

January 2023,

Decision on the substance 15/2023/2023 - 24/35

take organizational measures to ensure and be able to demonstrate that the

processing takes place in accordance with the GDPR. The defendant must do so

effectively implement data protection principles, the rights of data subjects

as well as only process personal data that is necessary for each

specific purpose of the processing.

II.4.1. Findings in the Inspection Report

85. Based on its investigation, the Inspectorate concludes that the
the defendant's privacy statement was not transparent and understandable to the defendant
data subjects as imposed by Article 12 (1) GDPR and from the point of view of
data protection contained irrelevant and incorrect information. Different elements
in the privacy statement were superfluous because it does not have the protection of
personal data went. Second, created the defendant's privacy statement
wrongly the perception to the data subject that the defendant fully complies with the GDPR
complied with, quod non, according to the Inspectorate. Thirdly, the privacy statement stated
wrong that the data subject always had to prove his identity in order to exercise
the rights of data subjects in the GDPR. This was incorrect because the defendant complied
Article 12 (6) GDPR may only request additional information from the data subject when he
has reasons to doubt the identity of the natural person making the request
submit as intended
in articles 15 up to and including 21 GDPR. Fourth, the
the defendant's privacy statement wrongly does not provide the opportunity for the data subjects
to submit a complaint to the Data Protection Authority. Finally, the
the defendant's privacy statement is not clear and therefore not transparent to the
stakeholders with regard to the interchangeable use of the terms
“personal data” and “data”, the purposes and legal bases of the processing, the
transfer of personal data and the adjustments that have been made.
86. In addition, the defendant's privacy statement was, according to the findings of the
Inspection service, incomplete because not all mandatory according to Articles 13 and 14 of the GDPR
information to be disclosed was effectively disclosed. After all, no information was included
about the contact details of the
data protection officer, de
processing purposes and the legal basis for the processing, the recipients or the

categories of recipients of the personal data, the storage period or the criteria for

determination of that period, the right of the data subject to limitation of the him

regarding processing as well as the right to data portability,

the right to withdraw a given consent and the right to lodge a complaint

to the Data Protection Authority.

II.4.2. Defendant's position

87. . With regard to these findings, the defendant argues that a new privacy policy

was worked out. At the time of drawing up the conclusion, the proposal was with the services

ICT and Communication for review. The implementation took place on March 18, 2022.

With regard to the privacy statement, the defendant argues that it has been updated

to comply with the findings of the Inspectorate. So became irrelevant

passages omitted, so that the statement is left with only the

relevant provisions

contains in accordance with the GDPR (principles of processing, purposes, legal basis,

data transfer, rights of data subjects and contact and complaint options

The involved). The defendant no longer automatically demands proof of identity

prior to exercising the data subject's rights. This will only be requested

when the identity of the data subject cannot be ascertained in any other way

insured. The privacy statement has also been supplemented with the various options available

the data subject has to file a complaint in the event of a possible violation of the

protection of his personal data. The privacy statement now also uses

consistent wording and to clarify the grounds for processing

specific examples are included, according to the defendant. In addition, the

privacy statement under the title “History of changes” next to the date of revision

also the subjects that have been effectively adapted. Finally, the defendant points out that

following information has been added to the privacy statement: contact details of the

data protection officer, purposes for processing, legal basis for

the processing, mention that only the defendant acts as controller and the

receives data, stating that the defendant no longer has the data in principle

than necessary for the purpose for which it was collected, the rights of the

data subjects and the complaint options of the data subjects. The defendant is therefore of

believes that the information it provides to data subjects meets the requirements of

Articles 12, 13 and 14 of the GDPR

II.4.3. Review by the Litigation Chamber

88. The Litigation Chamber points out that the GDPR determines which information must be mandatory

included in the privacy statement, and more specifically in articles 13 and 14 GDPR. This

Transparency requirements are further explained in the Transparency Guidelines

in accordance with Regulation (EU) 2016/679 of the Data Protection Working Party.

89. Since the defendant carries out a large number of data processing operations, resulting in a

large amount of

information must be provided to the data subjects,

is the

Decision on the substance 15/2023/2023 - 26/35

Litigation Chamber is of the opinion that a controller such as the defendant has a

multi-layered approach: 30

- On the one hand, the data subject must have clear and

accessible information about the fact that there are information about the processing of

personal data exists (privacy policy) and where he will be able to do it in full

find.

- On the other hand, without prejudice to the accessibility of the

privacy policy

in

its entirety, from the first

communication of the

controller with him be informed of the

details of the purpose of the processing in question, the

identity of the

controller and the rights available to him.

90. The importance of providing this multi-layered information ensures accessible and

comprehensible information for the data subjects, an obligation arising in particular from

recital 39 of the GDPR. All additional information within the meaning of Articles 13 and 14 GDPR that

necessary to enable the data subject on the basis of the information provided at this first level

information to understand what the consequences of the processing in question will be for him,

must be added.

91. The Litigation Chamber consulted the current privacy statement of the defendant and stated

confirming indeed that the latter has been updated in such a way as to take into account

took into account most of the comments of the Inspectorate and the

privacy statement was therefore almost completely aligned with the

relevant provisions of the GDPR. The Disputes Chamber takes note of this.

92. It is noted, however, that the new privacy statement does not yet address this

arrived at all the findings of the Inspectorate.

93. First of all, the Disputes Chamber notes that the privacy statement does not state clearly

makes of the retention periods of the personal data concerned or the criteria for

provision thereof, as required by Article 13 (2) a) GDPR. The privacy statement states

the following in this regard: “In principle, [we] do not store your data longer than

is necessary for the purpose for which it was collected. Being a government agency

however, we are often required by law to keep your personal data longer, under

more on the basis of archival legislation. It is also possible that your personal data

further processed for scientific and historical research or statistical purposes

purposes". However, the Guidelines of the Data Protection Group show that

30 In the same vein: Decision No 81/2020 of the Litigation Chamber (points 53 et seq.) and Decision 76/2021 (points 58

e.v.),

web page

https://www.dataprotectionauthority.be/professioneel/publicaties/besluiten.

available

through

the

such formulation is not sufficient. The Data Protection Group points out in this regard

note that the (mention of the) retention period is related to the principle of minimum

data processing covered by Article 5 (1) c) GDPR as well as the requirement of storage limitation

of Article 5(1)(e) GDPR. It specifies that “the storage period (or the criteria for

determine) may be dictated by factors such as legal requirements or sectoral

guidelines, but should always be formulated in such a way that the data subject, on the basis

of his or her own situation, can assess the retention period for specific

data/purposes”.31 The Disputes Chamber is of the opinion that this constitutes a violation

means of Article 13 (1) c) and 14 (2) c) GDPR.

94. Secondly, the Disputes Chamber notes in this context that the privacy statement is not op

mentions in sufficient detail the exact legal basis(s) and

purposes of the processing and which personal data are used for this purpose

personal data concerned, as required by Articles 13 and 14 GDPR. The Dispute Room

notes that the privacy statement does mention these elements, but that the way in which

is not understandable and transparent to the data subjects, as it is not clear to the

data subject which data are processed for which purpose and on what basis

legal basis this happens. Ideally, the controller provides a list

of the different purposes for which he processes personal data, with each time the

indication of which (categories of) personal data are processed for this purpose, via which

source they were obtained, for how long they are kept and with what (categories of)

recipients they (may) be shared.

95. The Disputes Chamber notes that the other findings of the Inspectorate

meanwhile was met by the amendments made by the defendant

to the privacy statement, but notes, however, that these findings at the time of the

performance of the inspection investigation are indisputable. The Disputes Chamber points it out

note that the defendant has made efforts to obtain the compensation under the

Articles 12, 13 and 14 GDPR to adjust the information to be provided, albeit after receipt

of the Inspectorate's comments.

96. The Litigation Chamber deduces from the findings of infringements listed above that the

defendant's transparency obligations under Article 12 GDPR and its information obligation

from Articles 13 and 14 GDPR has not been complied with. In doing so, the defendant has acted negligently

acted in breach of his accountability as set out in Article 5(2) and (24) of

the GDPR.

31 Transparency Guidelines under Regulation (EU) 2016/679, WP260rev1 adopted at 29

Nov. 2017, p 25.

II.5. Article 30, paragraph 1, paragraph 3 and paragraph 4 of the GDPR

97. In order to effectively apply the obligations contained in the GDPR, it is of

It is essential that the controller (and the processors) have an overview

of the processing of personal data that they carry out. So this registry is

primarily a tool to assist the controller in the

compliance with the GDPR for the various data processing operations it carries out because it

register makes its main features visible. The obligations regarding this

register of processing activities are defined in Article 30 GDPR.

98. Pursuant to Article 30 GDPR, each controller must keep records

of the processing activities carried out under its responsibility.

Article 30(1)(a) to (g) GDPR stipulates that, with regard to the

processing operations carried out by the controller, the following

information

must be available:

a) the name and contact details of the controller and any

joint controllers and,

where appropriate, of the

representative of the controller and of the officer for

data protection;

b) the processing purposes;

c) a description of the categories of data subjects and of the categories of

personal data;

d) the categories of recipients to whom the personal data have been or will be

provided, including recipients in third countries or international organisations;

e)

where applicable, transfers of personal data to a third country or a

international organisation, including the reference to that third country or countries

international organization and, in the case of the organizations referred to in Article 49(1) second subparagraph GDPR,

such transfers, the documents concerning the appropriate safeguards;

f)

if possible, the intended time limits within which the various categories of

data must be erased;

g)

if possible, a general description of the technical and organizational

security measures as referred to in Article 32 (1) GDPR.

99. The processing register must be in written form, including in electronic form,

be drawn up (Article 30(3) GDPR). In accordance with Article 30 (4) GDPR, the

controller the processing register

available to the

supervisory authority at its request.

100. With regard to the register of processing activities, the Inspectorate notes that

the defendant does not have the obligations imposed by Article 30 (1), (3) and (4) GDPR

complied. The Inspectorate has

after all, only part of the register of

receive processing activities, namely the building maintenance part.

The part that was transferred meets the requirements of the Inspectorate

does not meet the minimum requirements from Article 30 paragraph 1 GDPR as the following are mandatory

entries are missing:

a. The contact details of the defendant (Article 30(1)(a) GDPR).

b. A description of the categories of data subjects and of the categories of

personal data (Article 30(1)(c) GDPR). There is a short general summary

provided, but that is not a description, according to the Inspectorate.

101. The Litigation Chamber must rule on whether Article 30(1)(c) GDPR requires

that a description is given of the categories of personal data and the

categories of data subjects in the register of processing activities, or whether a

summary will suffice.

102. With regard to the lack of protection of the categories of data subjects and

personal data, the defendant asks for clarification in its conclusions. There are

indeed general examples are included in this regard, but the defendant states that

they do give an idea of the type of data that is meant. In the GDPR, the

Defendant cannot find a definition of what a description should be.

103. The Litigation Chamber notes that Article 30(1)(c) GDPR requires that a description of the

categories of data subjects and of the categories of personal data

included

in the register of processing activities. Those involved are the

identified or identifiable natural persons whose data are collected

processed (Article 4 (1) of the GDPR). As for the categories of data, of course it has to

concern personal data as defined in Article 4 (1) of the GDPR.

104. The Litigation Chamber

finds that the defendant

in service

registry of

processing activities enumerates:

- the categories of data subjects (Article 30(1)(c) GDPR), i.e. “staff members”.

- the categories of personal data (Article 30(1)(c) GDPR), namely the “Data

Geolocation system [...]: number plate, route traveled, vehicle description”.

105. The Litigation Chamber recalls the purpose of the

registry of

processing activities. To effectively fulfill the obligations contained in the GDPR

apply, it is essential that the controller (and the

processors) have an overview of the processing of personal data that they

to carry out. This registry
also is
primarily one
instrument to
assist the controller in GDPR compliance for the various
data processing operations that it performs because the register has its main features
makes visible. The Disputes Chamber is of the opinion that this processing register is a
is an essential tool in the context of the accountability already mentioned (Article 5,
paragraph 2, and Article 24 GDPR) and that this register forms the basis of all obligations that the
GDPR imposes on the controller.

106. Regarding the mandatory information pursuant to Article 30(1)(c) GDPR regarding the
description of the categories of data subjects and of the categories of
personal data, the Disputes Chamber notes that neither the text of the GDPR nor the
objectives of the GDPR prevent an enumeration of the categories of
personal data and the categories of data subjects is included in the register
processing activities or whether a more detailed description would be required.

107. With regard to the categories of recipients, the Litigation Chamber refers to a
recommendation of the CPP32 and the doctrine33 which sets out that although it is not
it is necessary to state the individual recipients of the data, but that they are
can be grouped by recipient category. Mutatis mutandis can do this
statement can also be applied to the categories of personal data and data subjects.
The Disputes Chamber hereby emphasizes that the information about the categories of
personal data and data subjects must be such that in the event of an exercise
of the right of access by a data subject, the controller specific
must be able to provide information to this data subject about the exact data processed
data and the specific recipients of its personal data.34

108. However, the Disputes Chamber points out that the

completion of the register

processing activities must always be evaluated on a case-by-case basis to determine whether the

description or enumeration contained herein is sufficiently clear and concrete. In this

case, the Disputes Chamber states that the description "personnel" is clear, since this

file shows that it concerns the employees of the Maintenance Buildings service. Also the

enumeration of the data generated by the software of the geolocation system

processed are clear. Consequently, the Litigation Chamber finds that in this case the above-mentioned

enumerations comply with the requirements of Article 30 (1) (c) GDPR.

109. As regards the missing entries from Article 30(1)(a) GDPR, the

Litigation room

determined that the

contact details

of the

officer

for

32 Available at: https://www.dataprotectionauthority.be/publications/aanbeveling-nr.-06-2017.pdf

33 W. Kotschy, "Article 30: records of processing activities", in Ch. KUNER The EU General Data Protection Regulation

(GDPR), a commentary, 2020, pg. 621.

34 ECJ, 12 January 2023, Österreichische Post AG, C-154/21, ECLI:EU:C:2023:3, para 36.

data protection are included in the modified version of the register

processing activities. This does not alter the fact that there was a historic breach of Article 30,

paragraph 1, a) GDPR and that it has been remedied in the meantime.

110. As regards the transmission of the register of processing activities, the

defendant does not that it was not submitted to the Inspectorate in its entirety. This

after all, the register of processing activities consists of several excel files, te
know one document per government department and it was reasoned by the defendant that
only the processing register of the service concerned had to be submitted. The
In its conclusions, the defendant declares that it is willing to submit the complete register of
processing activities, and has done so prior to the
hearing. The Disputes Chamber cannot deduce from further correspondence that the
Inspectorate would have requested these additional sheets.

111. The Disputes Chamber is of the opinion that the defendant has timely filed the processing register in the
particularly with regard to the geolocation system at issue
electronic form by e-mail at the first request of the Inspectorate. The additional
sheets were not further requested by the Inspectorate. Consequently, the
Litigation Chamber that there is no violation of Article 30, paragraphs 3 and 4 GDPR. However, there was one
historical infringement as regards Article 30(1)(a) of which the Litigation Chamber finds
that it was remedied by remedial measures.

II.6. Article 38(1) and (3) GDPR and Article 39(1) GDPR

112. The GDPR recognizes that the data protection officer is a key figure for what
concerns the protection of personal data whose designation, position and duties comply with rules
to be subjected. These rules help the controller to comply with
its obligations under the GDPR, but also help the
officer for
data protection to properly perform its tasks.

113. Article 38(1) GDPR requires the controller to take care of it
that the data protection officer is involved in a timely and appropriate manner
all matters related to the protection of personal data.

114. In addition, Article 38,
paragraph 3,

in

fine AVG that the

officer for

data protection reports directly to the top management

within the organization concerned. In addition, the data protection officer can

to report annually on the activities carried out by him and this ter

available to top management.

115. The Inspectorate finds that the defendant has fulfilled the obligations imposed by Article 38,

has not complied with paragraphs 1 and 3 GDPR. According to the Inspectorate, the defendant does not show

Decision on the substance 15/2023/2023 - 32/35

that its data protection officer has been properly and timely involved

in the context of the complaint. In addition, the defendant does not demonstrate that his

data protection officer reports effectively to the highest

managerial level of the defendant.

116. The Respondent does not dispute that it is of crucial importance that the official for

data protection is involved as early as possible in all matters related to

data protection related. Efforts have been made to this end

awareness of it, among other things, at the heads of department meeting of 3 December 2021. Brings further

the data protection officer will formally advise the data protection officer if necessary

Municipal Council/Social Welfare Council and/or the Municipal Executive

and Aldermen, this concerns 5 formal recommendations in 2021. The defendant also prepares documents

on demonstrating that the data protection officer is proactive,

such as 44 informal opinions in 2021. Finally, the defendant indicates that the annual report ter

notification is placed on the agenda of the Board of Mayor and Aldermen and the

Fixed desk.

117. In view of the above, the Disputes Chamber finds that the officer for

data protection is involved on a regular basis in matters with

regarding the protection of personal data. Specific as to the context of

the complaint, the Disputes Chamber notes that the officer was involved in the run-up to

the present complaint. The complaint was filed on March 31, 2021 after being filed on November 16

2020 and on 23 February 2021, there was consultation between the defendant and the officer

for data protection on the geolocation policy. From the whole of all the pieces that

were submitted, are no concrete elements that allow the Disputes Chamber to

conclude that the data protection officer would not be involved in a timely manner

have been. However, the Litigation Chamber points out that documenting the timely

involvement can be useful for the controller itself, but also for the

Inspectorate in the event of a complaint, as well as during the (casuistic) assessment by the

Litigation room.

118. The Inspectorate also found an infringement of Article 38(3) regarding the

reporting to the highest management level. The defendant had during the

research

clarified

On

the

Inspection Service

that

the

officer

for

data protection chairperson of the Information Security Cell, which reports

to the General Manager via the annual report. The Inspectorate refers in this regard

to an earlier decision of the Litigation Chamber in which it was clarified that in a

municipality the college of mayor and aldermen the highest daily

managerial level. The Disputes Chamber notes that in the course of October to

December 2020 has an audit of the defendant carried out by Audit Vlaanderen

Decision on the substance 15/2023/2023 - 33/35

occurred. This included a recommendation that the defendant has

its own framework for organizational management, which includes reporting to the Executive Board

Mayor and Aldermen foresees this

lacking in practice. The

The Disputes Chamber notes that the defendant has set to work with this recommendation

since in 2021 5 formal and 44 informal recommendations will be made directly to the Executive Board

Mayor and Aldermen were addressed, in addition to the annual report that the official for

data protection issues annually.

119. Based on the above, the Disputes Chamber concludes that there is no infringement of

Article 38 (1) and (3) and Article 39 (1) GDPR. This does not alter the fact that it is historical

has been an infringement with regard to Article 38 (3) GDPR and that this has been done by remedial

measures were remedied.

III. Sanctions

120. On the basis of the documents in the file, the Disputes Chamber establishes that there is

following (historical) infringements:

-

Article 5 (1) (a) and (2) and Article 6 (1) GDPR, and Article 24 (1) and Article 24 (1) and (2) of

the GDPR with regard to the geolocation system;

-

Article 4, 11), Article 5(1)(a) and (2), Article 6(1)(a) and Article 7(1) and (3) for what

concerns the use of cookies that are not strictly necessary;

-

Article 12(1) and (6), Article 13(1) and (2), Article 14(1) and (2), Article 5(2), Article 24(1)

and Article 25 (1) GDPR with regard to the information obligations;

-

Article 30 (1) (a) GDPR with regard to the contact details of the officer in the

register of processing activities; and

-

Article 38, paragraph 3 GDPR with regard to direct reporting to the highest

managerial level.

121. While the Respondent has taken remedial action to rectify these infringements whether or not

not already completely remedied, it is certain that there are infringements of the right to

data protection have taken place. As already explained are the principles

of legality and transparency fundamental principles of the GDPR. Also the

data protection officer plays a vital role in data protection

to a controller. The Litigation Chamber reminds that the AVG already

entered into force in 2016, and became applicable on 25 May 2018. In the meantime, almost

5 years have passed since the GDPR became applicable, a period specified by the defendant

has been insufficiently used to make its operation GDPR-compliant.

122. When determining the sanction, the Disputes Chamber takes into account the fact that the

the defendant has already (partially) rectified these infringements and evidence thereof

Decision on the substance 15/2023/2023 - 34/35

transfers. Needless to say, the Disputes Chamber points out that it is not authorized to

impose an administrative fine on public authorities, in accordance with Article 221,

§ 2 of the Data Protection Act.35 In view of the above, the Litigation Chamber

is of the opinion that a reprimand based on Article 100, § 1, 5 WOG is appropriate in this case

is.

123. The Disputes Chamber proceeds to dismiss the other grievances and findings of the

Inspectorate because, based on the facts and the documents in the file, they do not belong to the

conclude that there has been a breach of the GDPR. These grievances and

findings of the Inspectorate are therefore regarded as manifestly unfounded

within the meaning of Article 57(4) of the GDPR.36

IV. Publication of the decision

124. Given the importance of transparency with regard to decision-making by the

Litigation Chamber, this decision will be published on the website of the

Data Protection Authority. It

however, it is not necessary that the

identification data of the parties are disclosed directly.

FOR THESE REASONS,

the Disputes Chamber of the Data Protection Authority decides, after deliberation, to:

- on the basis of Article 100, §1, 5° WOG to formulate a reprimand with regard to the

defendant for the infringement of Article 5(1)(a) and (2) and Article 6(1);

Article 24(1) and Article 24(1) and (2); Article 4, 11), Article 5(1)(a) and (2), Article 6(1)(a)

and Article 7(1) and (3); Article 12(1) and (6), Article 13(1) and (2), Article 14(1) and (2),

Article 5 (2), Article 24 (1) and Article 25 (1) GDPR; Article 30 (1) GDPR and Article 38 (3)

GDPR;

- pursuant to article 100, §1, 1° WOG with regard to all other determinations in

dismiss.

Pursuant to Article 108, § 1 of the WOG, within a period of thirty days from the

notification against this decision may be appealed to the Marktenhof (court of

Brussels appeal), with the Data Protection Authority as defendant.

35 Law of 30 July 2018 on the protection of natural persons with regard to the processing of

personal data, B.S., September 5, 2018.

36 See point 3.A.2 of the Dispute Chamber's Dispute Policy, dd. 18

June 2021, te

https://www.dataprotectionauthority.be/publications/sepotbeleid-van-de-geschillenkamer.pdf

consult via

Decision on the substance 15/2023/2023 - 35/35

Such an appeal may be made by means of an inter partes petition

must contain the information listed in Article 1034ter of the Judicial Code37. It

a contradictory petition must be submitted to the Registry of the Market Court

in accordance with Article 1034quinquies of the Ger.W.38, or via the e-Deposit

IT system of Justice (Article 32ter of the Ger.W.).

(get.) Hielke HIJMANS

Chairman of the Litigation Chamber

37 The petition states under penalty of nullity:

1° the day, month and year;

2° the surname, first name, place of residence of the applicant and, where applicable, his capacity and his national register or

3° the surname, first name, place of residence and, if applicable, the capacity of the person to be

enterprise number;

summoned;

4° the object and brief summary of the means of the claim;

5° the court before which the action is brought;

6° the signature of the applicant or his lawyer.

38 The petition with its annex is sent, in as many copies as there are parties involved, by registered letter

sent to the clerk of the court or deposited at the clerk's office.