1/20

Litigation Chamber

Decision on the merits 16/2020 of 20 April 2020

File number: DOS-2018-04918

Subject: Complaint against a store regarding the use of surveillance cameras

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

Hijmans, chairman, and Messrs. Yves Poullet and Christophe Boeraeve, members. The case is

resumed in its current composition.

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 GDPR;

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

Having regard to the Law of March 21, 2007 regulating the installation and use of surveillance cameras (hereinafter the

Cameras Act);

Having regard to the internal rules of the Data Protection Authority as approved by the

Chamber of Representatives on December 20, 2018 and published in the Belgian Official Gazette on January 15, 2019;

Considering the documents in the file;

Decision on the merits 16/2020 - 2/20

Made the following decision regarding:

-

-

the complainant:

the data controller (hereinafter the defendant)

I.

Feedback from the procedure

Having regard to the complaint filed on September 9, 2018 by the complainant with the Authority for the Protection of data (ODA);

Considering the decision of October 5, 2018 of the Front Line Service (SPL) of the APD declaring the complaint admissible and the transmission of it to the Litigation Chamber on the same date;

Having regard to the decision taken by the Litigation Chamber during its session of October 23, 2018 to refer the file to the Inspectorate under article 96, § 1 LCA, of which the complainant was informed by letter of the same date;

Having regard to the Inspector General's investigation report of May 14, 2019;

Having regard to the decision taken by the Litigation Chamber during its meeting of May 28, 2019 to consider that the case was ready for substantive processing under Articles 95 § 1, 1° and 98 LCA;

Having regard to the letter dated May 29, 2019 from the Litigation Chamber informing the parties of its decision to consider the file as being ready for substantive processing on the basis of article 98 LCA and communicating the inspection report to them;

Given the request made by the defendant on June 25, 2019 to be, following the exchange of conclusions, heard by the Litigation Chamber pursuant to Article 51 of the Rules of Procedure domestic ODA;

Having regard to the letter of June 26, 2019 from the complainant in which he puts forward his arguments;

Having regard to the submissions in response of the defendant filed by its counsel, received on July 30, 2019;

Having regard to the complainant's letter of July 31, 2019;

Having regard to the invitation to the hearing sent by the Litigation Chamber on February 6 and March 4 2020;

Having regard to the information on the holding of a hearing provided to the Inspector General pursuant to Article 48 paragraph 2 of the Internal Rules of the Data Protection Authority dated 27 February and March 9, 2020;

Having regard to the hearing during the session of the Litigation Chamber of March 13, 2020 in the presence of the defendant and his counsel;

Having regard to the minutes of the hearing;

Having regard to the observations communicated by the defendant on the minutes of the hearing on March 21 2020 which were attached to the minutes and sent for information to the complainant on 23 March 2020 (article 54 of the DPA's internal rules).

Having regard to the observations communicated by the complainant on the minutes of the hearing on March 26, 2020, which were attached to the minutes and transmitted for information to the defendant on April 15 2020 (article 54 of the DPA's internal rules)

II.

The facts and the subject of the complaint

In his complaint of September 9, 2018, the complainant complains that on September 4, 2018, he was filmed by a camera as he walked on the sidewalk alongside the defendant's store. He says he saw himself on a television screen hanging on the back wall of the store, across the shop window in question.

Under the terms of his complaint, the plaintiff indicates that he was filmed by “360° globe” cameras without his consent in disregard of his image rights and more generally of the regulations applies. He presumes that these images were recorded and denounces the absence of pictogram at the date of September 4, 2018 on the shop windows informing passers-by of the presence of cameras.

III.

The inspection report of May 14, 2019

As part of his Inspection, the Inspector General asked the defendant to provide him with the following information and to send him the relevant documents in support thereof (mail of the Inspector General of April 4, 2019):

- Detailed information on the use of surveillance cameras by the defendant

in the street; the storage of camera images (storage period and location of the

physical and technical storage of data), any subcontractors who are

responsible for controlling camera images under the authority of the data controller;

- Details on the delimitation of the place filmed and the possible adjustments that the defendant

has planned to exclude the fact of filming passers-by in the street, this could for example be

provided by screenshots of camera images;

Proof of the declaration of the installation and use of a monitoring system by

-

cameras electronically via the centralized electronic reporting window for

camera surveillance systems, made available by the Federal Public Interior Service;

- A copy of the register listing the image processing activities of security cameras

surveillance of the defendant;

Proof of the affixing of a pictogram by the defendant indicating the existence of a

-

camera surveillance.

At the end of its analysis and in support of the information and documents obtained both from the complainant and from

respondent, the Inspector General concludes in his report of May 14, 2019 with the following findings:

-

“The surveillance cameras have not been the subject of a declaration as such to

of the Commission for the Protection of Privacy (hereinafter CPVP) prior to their implementation

in service. They have now been declared to the police since 10/05/2019.

-

The record of processing activities contains only one one-time processing dated

27/12/2018. The processing of video surveillance in a closed place accessible to the public is not

not included in the register”.

IV.

The hearing of March 13, 2020

The defendant began the hearing on March 13, 2020 - a detailed report of which was drawn up and

communicated to both parties - by enlightening the Litigation Chamber on the context in which the

complaint has been filed. She explained in particular that the complainant often visited a person

living in the building on the ground floor of which the defendant has its offices, person with whom

the defendant stated that it had difficult neighborly relations. The defendant clarified

that the conflict with the plaintiff arose when she wanted to install her security cameras

external surveillance, installation following which the complainant seized several bodies, including

the Data Protection Authority

The defendant expressly admitted having made an error with regard to the declaration of the

surveillance cameras at the OPC in April 2018. The defendant wrongly believed that the process

declaration was complete when she printed the declaration she had just completed. In

In reality, only one project was in the system. This project should have been referred to the CPP in order to be able to

consider that the declaration process was finalized, which was not done.

Asked about the register of processing activities (Article 30 of the GDPR and Article 6 § 2 al. 4 of

the Cameras Law), the defendant referred to its conclusions of July 30, 2019, according to which

she indicates that as part of the inspection, she attached “a copy of the register of activities of

processing drawn up on the basis of the model established by the Autorité” (page 3 of the conclusions). At the end of the

explanations received during the hearing regarding these registers and their content, the defendant

committed to creating a register of its processing activities (see the observations communicated on

March 21, 2020 by the defendant on the minutes of the hearing of March 13, 2020).

PLACE

v.

Preliminary remark

As a preliminary point, the Litigation Chamber finds that the plaintiff deliberately did not wish

communicate its arguments to the defendant, even though in its registered letter

of May 29, 2019, the Litigation Chamber expressly requested it. In this letter, the

Litigation Chamber informs the parties that the case is ready for substantive processing in

application of Article 98 LCA and that each of them is required to simultaneously transmit its

conclusions to the secretariat of the Litigation Chamber and to the other party.1 The Litigation Chamber

notes that the complainant indicated that he believed that it was up to the Litigation Chamber to make this

communication of its arguments to the defendant.

In his letter of June 26, 2019, the complainant wrote: “From the outset, I would like to specify that,

as a citizen whose privacy must be respected and protected, he is extremely against

indicated that I am relaying my findings directly to other parties but I am waiting for this to happen.

do by your steps".

Notwithstanding the lack of communication by the complainant of his arguments of June 26, 2019 to the

defendant in violation of the rights of the defence, the Litigation Division notes however that

during the communication on July 11, 2019 of a copy of the file requested by the defendant,

1 This obligation arises from Article 50 of the Internal Rules of the Data Protection Authority.

this letter from the complainant dated June 26, 2019 was part of the disclosed record. The defendant has

so could learn about it.

On the other hand, the Litigation Chamber notes that on July 31, 2019, the complainant reacted to the

conclusions of the defendant of July 30, 2019, and this outside the timetable established by the Chamber

Litigation in its aforementioned letter of May 29, 2019 and without informing the defendant. The

Chambre Litigation will take no account of this letter, which, moreover, does not contain

nothing relevant to this decision.

VI.

As to the competence of the Data Protection Authority, in particular

of the Litigation Chamber

Pursuant to Article 4 § 1 LCA, the Data Protection Authority (DPA) is responsible for the

monitoring compliance with the data protection principles contained in the GDPR and other laws

containing provisions relating to the protection of the processing of personal data

including the Law of 21 March 2007 regulating the installation and use of surveillance cameras (Law

cameras).

Pursuant to Article 33 § 1 LCA, the Litigation Chamber is the litigation body

ODA administration. It is seized of the complaints that the Service de Première Ligne (SPL) forwards to it.

pursuant to Article 62 § 1 LCA, i.e. admissible complaints provided that in accordance with

article 60 paragraph 2 LCA, these complaints are written in one of the national languages, contain a

statement of the facts and the indications necessary to identify the processing of personal data

personnel to which they relate and fall within the competence of the DPA.

This administrative nature has been confirmed by the Court of Markets, the court of appeal for decisions

of the Litigation Chamber. 2

The Litigation Chamber is not competent to condemn the plaintiff or any party to the

cost proceedings. Articles 95 and 100 LCA exhaustively list the corrective measures

and penalties it may decide. Order to pay costs is not one of the measures listed

in these articles, in particular to article 100 LCA applicable in the present case.

Overly, and insofar as necessary, the Litigation Chamber adds that the Code

judiciary, article 1022 of which provides for condemnation to costs, does not apply to the Chamber

Litigation in its capacity as a litigation body of an independent administrative authority except

2 See. in particular the judgment of 12 June 2019 of the Court of Appeal of Brussels, 19th chamber, section Court of Markets pu

the DPA website: https://www.autoriteprotectiondonnees.be/decisions-de-la-cour-des-marches

in cases where, as in Article 57 of the Internal Rules, the application of the provisions of the

Judicial Code is specifically provided.

The Litigation Division cannot therefore grant the defendant's request to condemn the

plaintiff to costs up to 1,440 euros. This request by the defendant made to the

terms of its conclusions of July 30, 2020 (page 9) is rejected.

In its conclusions, the defendant indicates that it notes that the complainant does not make any

own claim for compensation on the basis in particular of his right to the image and that in any case

case, it considers that the plaintiff suffered no personal prejudice (point 2.2.2.3. of the conclusions

of the defendant of July 30, 2019, page 8). In the operative part of its conclusions, the defendant

asks that in any event, the Litigation Chamber acknowledges that the

plaintiff does not make any specific claim for compensation as well as to note that the plaintiff

does not suffer any personal damage (page 9 of the defendant's conclusions of July 30, 2019).

The Litigation Chamber is not competent to grant any compensation. She does not

a fortiori not to establish the existence or not of prejudice on the part of the plaintiff.

The existence of prejudice on the part of the plaintiff is not, moreover, necessary to establish the claim.

jurisdiction of the Litigation Chamber.

VII.

On the reasons for the decision

On the defendant's breaches of its obligations under the Cameras and

GDPR

In its capacity as data controller, the defendant is required to respect the principles of

data protection and the obligations imposed on it by the GDPR and must be able to

demonstrate that these are respected (principle of responsibility – article 5.2. of the GDPR) and put in place

implement all the necessary measures for this purpose (Article 24 of the GDPR). Filmed image processing

by surveillance cameras is indeed, since these images constitute data to be

personal character, subject to the GDPR to be applied in parallel with the Cameras Law.

In addition to the GDPR, the defendant is indeed also required to comply with the obligations that the Law

cameras, also revised in 2017 to take into account the entry into force and entry into

future application of the GDPR, has been charged to it.

7

Decision on the merits 16/2020 - 8/20

The Litigation Chamber qualifies the cameras affixed by the defendant as cameras of

surveillance of a closed place accessible to the public within the meaning of article 2, 2° and 4° of the Cameras Act3

given the purpose of monitoring the security of the premises pursued by the installation of these

cameras.

 Regarding the declaration of surveillance cameras (article 6 § 2 al. 1 of the Cameras Law)

The Inspector General's report of May 14, 2019 points out that the surveillance cameras of the

defendant were not the subject of a declaration as such to the Commission of the

protection of privacy (CPVP) prior to their commissioning,

Pursuant to Article 6 § 2 of the Cameras Law as applicable until May 25, 2018, the

controller had to notify its decision to install surveillance cameras in a

closed place accessible to the public to the Commission for the protection of privacy and to the head of the body

of the police zone where the place was located4.

This lack of declaration is not disputed by the defendant or in the terms of its conclusions.

of July 30, 2019 (see below) nor in the terms of his remarks during the hearing of March 13, 2020.

The defendant indeed admits on page 8 of its conclusions of July 30, 2019 that “the only

breach which could be attributed to the conclusive [read the defendant] is to have considered

unintentionally that the declaration transmitted to the DPA was worth proof of a declaration”.

The Litigation Chamber notes that this draft declaration form is dated April 24, 2018

(page 2 of the Inspection report of May 14, 2019), be completed in tempore non suspecto, the facts

denounced by the plaintiff dating them from September 4, 2018.

In his investigation report, the Inspector General indicates in this regard that “the form relating to the

statement sent by the store manager does not constitute proof of a statement in

as such with the Commission for the Protection of Privacy (as is clearly specified

in the preamble of the form). It appears from a check in the archives of the declarations at

the Privacy Commission that the form has not been sent to the Commission

3 Art. 2. For the purposes of this law, the term (…) means: 2° closed place accessible to the public: any building

or place bounded by an enclosure]2 intended for the use of the public, where services can be provided to it.

4 Article 6 of the Cameras Law of March 21, 2007:

§ 1. The decision to install one or more surveillance cameras in a closed place accessible to the public is

taken by the controller.

§ 2. The controller notifies the decision referred to in § 1 to the Commission for the Protection of Life

private4 and to the commander of the police zone where the place is located. He does this no later than the day before the day

commissioning of the surveillance camera(s).

of the protection of privacy. The declaration is therefore not complete (…)” (page 3 of the report

Inspection of May 14, 2019).

The Litigation Chamber is not competent to hear breaches that would be

prior to May 25, 2018, the date of entry into force of the Law establishing the Authority

data protection.

The Inspection report goes on to state that these cameras are now declared to the

police services since May 10, 2019. This statement is produced by the defendant

(page 4 of the Inspection report of May 14, 2019).

According to article 6 § 2 al. 1 of the Cameras Law of March 21, 2007, the data controller

notifies the police services of its decision to install one or more surveillance cameras in a

closed place accessible to the public. This notification must be made no later than the day before the day of the

in service of the surveillance camera.

The Litigation Chamber notes that on the date of the facts denounced in the complaint (i.e. September 4

2018), this statement had not been made to the police. The defendant, subsequently

to the complaint lodged by the complainant and the intervention of the Inspection service, regularized the

situation by declaring its surveillance cameras to the police on May 10, 2019.

Given the absence of a declaration to the CPP before May 25, 2018, even following a

misunderstanding on the part of the defendant as to the finalization of the procedure by

the sending of the form of April 24, 2018 mentioned above, the defendant cannot invoke article 89

of the Law of March 21, 2018 amending the law on the police function, with a view to regulating the use of cameras

by the police services, and amending the law of March 21, 2007 regulating the installation and use of

surveillance cameras, the law of 30 November 1998 on the organization of intelligence and

security and the law of October 2, 2017 regulating private and particular security.

This article 89 specifies that as of May 25, 2018, surveillance cameras regulated by the Law of

March 21, 2007 regulating the installation and use of surveillance cameras, installed and used

in accordance with the legislation in force at the time of their installation, must comply with

the obligation to notify the police at the latest within two years. Bedroom

Litigation considers that the defendant cannot rely on it since it had not duly

declared its surveillance cameras to the CPP on May 25, 2018.

In conclusion, in view of the foregoing developments, the Litigation Chamber concludes that

breach of Article 6 § 2 al. 1 of the Law of March 21, 2007.

 The register of processing activities required by Article 30 of the GDPR and the register of

processing of images from surveillance cameras (article 6.2 al. 4 of the Cameras Law)

The register of processing activities required by Article 30 of the GDPR)

Under the terms of Article 30 of the GDPR, any data controller (subject to Article 30.5.

discussed further below) must keep a register of the processing activities carried out under its

responsibility.

Section 30.1. a) to g) of the GDPR provides that the information below must be available

in relation to the processing carried out in this capacity of data controller5. Bedroom

Litigation specifies that it is with regard to data processing that a certain number

information is required. The register of processing activities is, as its name suggests, a

processing register and not a register containing the personal data processed.

The register must have the following content:

-

the name and contact details of the data controller and, where applicable, of the controller

spouse of the processing as well as the representative and the data protection officer

possible (article 30.1.a) of the GDPR);

-

the purpose(s) (Art. 30.1. b) of the GDPR), they must be stated clearly and with

precision ;

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

-

personal data processed, with regard to each of the identified purposes (Art. 30.1. c) of the GDPR).

The Litigation Chamber recalls that the persons concerned are the persons

identified or identifiable individuals whose data is being processed (Art. 4 (1) GDPR). As to

to the categories of data, it must of course be personal data such as

defined in Article 4 (1) of the GDPR). Where applicable, the processing of personal data

referred to in Articles 9 and 10 of the GDPR must be identified without only "categories" of

data it is not necessary to understand only the data referred to in articles 9 and 10 of the GDPR and those

that would not come out of these articles;6

the categories of recipients to whom the data have been or will be communicated, including

-

including recipients in countries outside the European Union or organizations

5 See. section 30.2. of the GDPR for the content of the register to be kept by the processor and the recommendation

06/2017 of the CPP already cited.

6 For examples of categories, see. CPP Recommendation 06/2017 already cited.

international, with regard to each of the identified purposes (Art. 30.1. d) of the GDPR). Are

therefore targeted, both potential internal and external recipients (such as subcontractors or

third parties), established within or outside the European Union;

-

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

international organisation, including the identification of this third country or this organization

international. In the case of transfers referred to in Article 49.1. paragraph 2 of the GDPR, the documents

attesting to the existence of appropriate guarantees, with regard to each of the purposes

identified (Art. 30.1. e) of the GDPR), must also be referenced;

-

as far as possible, the deadlines provided for the erasure of the different categories of

data (Art. 30.1. f) GDPR). This piece of information is consistent with the principle of article 5.1.e)

of the GDPR, according to which the data cannot be stored in a form that allows

the identification of persons only for a period not exceeding that necessary for the

with regard to the purposes for which they are processed. For shelf life, do not

not necessarily include a duration in days, months, years, or an evaluation

necessarily quantitative. Shelf life can also refer to

parameters such as the time required to achieve the specific purpose pursued as well

as well as the management of any litigation relating thereto, the expiry of a limitation period, etc. ;

- As far as possible, a general description of the technical security measures and

organizational arrangements referred to in Article 32.1. GDPR (Art. 30.1. g) GDPR). Section 32.1. from

GDPR requires that the data controller and the processor implement the

appropriate technical and organizational measures to guarantee a level of security

adapted to the risk.

The Litigation Chamber considers that this register of processing activities is an essential tool

accountability, i.e. the principle of liability of the data controller already mentioned

(articles 5.2. and 24 of the GDPR) (as well as, indirectly, from the processor9) and who is the underlying

to all the obligations imposed on it by the GDPR.

Indeed, in order to be able to effectively apply the data protection rules

contained in the GDPR and the obligations imposed on them, it is essential that those responsible

processors (and processors) identify and have an overview of the processing of

personal data that they process.7 This register is therefore first and foremost a tool intended to help

7 Commission for the protection of privacy, Recommendation 06/2017 of 14 June 2017 relating to the register of

processing activities (article 30 of the GDPR):

controllers (and processors) to comply with the GDPR by viewing the different

data processing they carry out and their main characteristics.

Under the GDPR, this register is not intended for the public. It may, however, be useful both

data controller and, where appropriate, the data protection officer interviewed by

data subjects in the context of the exercise of their rights.

Consultation of the register must also be able to enable the supervisory authority to

account of the processing carried out and information relating to this processing. In execution of the article

30.4. of the GDPR, the data controller or the processor thus makes said register available to

available to the supervisory authority on request.

The language used in the Register must be clear and accessible and the register readable for the DPA.

The register of processing activities is a living tool, which will evolve according to the

development of the controller's activities. It must be constantly updated8.

The obligation to keep a register of processing activities is a dynamic obligation, in the sense

that the data controller and the processor will ensure that it is kept up to date by adding new

treatments carried out but also, with regard to treatments already listed, for example any new

recipient, any new categories of data processed, any change in the retention period

or modification of any other required piece of information.

The register must, from the date of entry into application of the GDPR, i.e. from May 25, 2018,

contain the elements of information required with regard to the processing carried out on this date, whether they are

operated for a long time or more recently.

This obligation applies to the defendant. As far as necessary, the Litigation Chamber

clarifies that Article 30.5. of the GDPR does not apply to the defendant since the latter

performs processing on a regular basis, which excludes any possibility for it to rely on

the exceptions provided for in Article 30.5. of the GDPR. The exceptional hypotheses provided for are not

cumulative and one of them providing that when the data processing carried out is not

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_06_2017.

pdf From 2017, i.e. during the period between the entry into force of the GDPR and its entry into force, the

Commission for the Protection of Privacy has published a recommendation explaining how it is appropriate

complete the register.

8 Commission for the protection of privacy, Recommendation 06/2017 of 14 June 2017 relating to the register of

processing activities (Article 30 of the GDPR).

not occasional the exception falls, the defendant cannot benefit from the exemption regime provided for

in section 30.5. GDPR..

Section 30.5. of the GDPR provides that “the obligations referred to in paragraphs 1 and 2 do not

do not apply to a business or organization with less than 250 employees, unless the

processing they carry out is likely to entail a risk for the rights and freedoms of

persons concerned ; if it is not occasional or if it relates in particular to the categories

specific data referred to in Article 9(1) or on personal data

relating to criminal convictions and offenses related to Article 10.”

If they are in one of the 4 hypotheses below - which are not cumulative -, the

companies and organizations, even if they have less than 250 employees, will therefore still have to

keep a record:

-

the processing they carry out is likely to entail a risk for the rights and

freedoms of data subjects9;

9 Recital 75 of the GDPR clarifies in this regard that: “Risks to the rights and freedoms of individuals

physical injuries, the likelihood and severity of which vary, may result from the processing of personal data

personnel that is likely to cause physical or material damage or moral harm, in

particular:

-

where the processing may give rise to discrimination, identity theft or theft,

financial loss, damage to reputation, loss of confidentiality of data protected by

professional secrecy, unauthorized reversal of the pseudonymization process or any

other significant economic or social harm;

-

when the data subjects could be deprived of their rights and freedoms or prevented

to exercise control over their personal data;

-

when the processing concerns personal data which reveals racial origin or

ethnicity, political opinions, religion or philosophical beliefs, trade union membership,

as well as genetic data, data concerning health or data concerning life

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

related security measures;

-

when personal aspects are assessed, especially in the context of analysis or prediction

elements relating to work performance, economic situation, health, preferences or

personal interests, reliability or behavior, whereabouts or movements, with a view to

create or use individual profiles;

-

The treatment they perform is not casual. Occasional treatment should be

understood as treatment that is such by occasion, chance, fortuitous, as opposed to

usual. Are for example not occasional processing, data processing

related to customer management, personnel management (human resources) or even

supplier management.

The processing they carry out relates to special categories of data in the article

9 GDPR (sensitive data).

The processing they carry out relates to data referred to in Article 10 of the GDPR (data

judicial).

-

-

In a document relating to the scope of this exemption provided for in Article 30.5. of the GDPR, the Group

of Article 29, states in the same sense as follows:

“Therefore although endowed with less than 250 employees, data controllers or processors

who find themselves in the position of either carrying out processing likely to result in a risk

[not just a high risk] to the right of the data subjects, or processing personal data on a non-

occasional basis, or processing special categories of data under article 9 (1) or data relating

to criminal convictions under article 10 are obliged to maintain the record of processing

activities”. (…) “For example, a small organization is likely to regularly process data regarding

its employees. As a result, such processing cannot be considered “occasional” and must

therefore be included in the record of processing”. 10

Translation:

"Therefore, although with less than 250 employees, data controllers or

subcontractors who find themselves in the situation either of carrying out processing likely

-

when the processing relates to personal data relating to natural persons

vulnerable, especially children; or when the processing involves a large volume of

personal data and affects a significant number of data subjects.

10 Working Party 29 Position paper on the derogations from the obligation to maintain records of processing

activities pursuant to Article 30(5), endorsed by the European Data Protection Board

(EDPB): https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf. See.

also: Dr W. Kotschy, Comment on Article 30 (Record of Processing Activities), in C. Kuner, L. A. Bygrave

and C. Docksey, The EU General Data Protection Regulation (GDPR): a commentary, Oxford University Press,

2020, p. 623.

cause a risk (not just a high risk) to the rights of individuals

concerned, either to process personal data on a non-occasional basis,

either to process special categories of data referred to in Article 9 (1) or data

relating to criminal convictions referred to in Article 10 are obliged to keep a register

processing activities".. (…) "For example, a small organization is likely to

regularly process data relating to its employees. Therefore, such treatment

cannot be considered as "occasional" and must therefore be included in the register

processing activities".

In this case, the record of the defendant's processing activities required by Article 30 of the GDPR

must include information relating to the image processing activities of surveillance cameras,

these being personal data within the meaning of Article 4.1. of the GDPR.

The register of surveillance camera image processing activities (article 6. 2 al. 4 of the

Camera law)

According to article 6. 2 al. 4 of the Cameras Law, the data controller keeps a register

taking over the surveillance camera image processing activities implemented under its

responsibility. This register is in written form, which may or may not be electronic. On

request, the data controller shall make this register available to the Data Protection Authority.

data and police services.

The content of this register is defined by the Royal Decree of 8 May 2018 relating to declarations

installation and use of surveillance cameras and the register of image processing activities

of surveillance cameras11, entered into force on May 25, 2018.

Article 7 of this royal decree defines the content of the register of image processing activities of

surveillance cameras by reference to article 30.1. of the GDPR described above12. This content is in

effect defines as follows:

1° the name and contact details of the controller and, where applicable, of the controller

spouse of the processing, the representative of the controller and the delegate for the

Data protection;

2° the purposes of the processing;

11 MB, 23 May 2018.

12 See. in this regard the opinion 24/2018 of March 21, 2018 of the Commission for the Protection of Privacy (CPVP)

relating to the draft royal decree relating to declarations of installation and use of surveillance cameras

and in the surveillance camera image processing activity register:

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_24_2018_0.pdf

15

Decision on the merits 16/2020 - 16/20

3° a description of the categories of data subjects and the categories of data to be

personal character;

4° the categories of recipients of the personal data, including the

recipients in third countries or international organisations;

5° where applicable, transfers of personal data to a third country or to a

international organisation, including the identification of this third country or this organization

international community and, in the case of transfers referred to in the second subparagraph of Article 49(1),

of the General Data Protection Regulation, the documents attesting to the existence

appropriate safeguards;

6° the deadlines provided for the erasure of the different categories of data, namely the deadline

data retention, if the images are saved;

7° a general description of the technical and organizational security measures referred to

to Article 32(1) of the General Data Protection Regulation, the

security measures taken to prevent access by unauthorized persons and those

which are taken in the context of the communication of data to third parties.

The Litigation Chamber recalls here that the register required by Article 30 of the GDPR must, in all

assumption, include information relating to the image processing activities listed in Article 7

of the Royal Decree implementing the aforementioned Camera Law (which are, as already mentioned,

directly inspired by the elements listed in article 30.1. GDPR)13.

In its opinion 24/2018 relating to the preliminary draft of this royal decree implementing the Cameras Act 14, the

CPVP had thus indicated "that the content of the register that a data controller must keep (...)

is generally determined by Article 30 of the GDPR and that the delegation to the King provided for in

preliminary draft to determine this content should preferably be limited to specific aspects which

are specific to data processing carried out using surveillance cameras."

Article 8 of the same royal decree adds that in addition to these elements listed in the aforementioned article 7, this register

image processing must contain:

1° the legal basis of the processing;

2° indication of the type of place;

3° the technical description of the surveillance cameras, as well as, in the case of

fixed surveillance, their location, if necessary indicated on a plan;

4° in the case of temporary or mobile surveillance cameras, the description of the areas

monitored by these surveillance cameras and the periods of use.

13 See. opinion 24/2018 of March 21, 2018 of the Privacy Commission already cited.

14 Same.

5° the mode of information about the processing;

6° the place where the images are processed;

7° the fact that real-time viewing is organized or not and, where applicable, the manner

which it is organized.

However, it is not necessary for the defendant to establish two separate registers. A register

unique can be established provided that it contains, with regard to the processing activities that are

listed, all the mandatory information – including therefore those which are specifically

required by article 8 of the Royal Decree of 8 May 2018 implementing the Cameras Law with regard to the activities of

image processing.

The findings of the inspection report and the hearing of March 13, 2020

The inspection report of 14 May 2019 concludes that the register of processing activities submitted by
the defendant following the request of the Inspector General of April 4, 2019 contains only one
only one-time treatment on 27/12/2018. CCTV processing in a place
closed accessible to the public is not included. In his email of April 12, 2019 to the inspection service,
the defendant writes in this respect “You will find attached the register; it is almost empty”.
Notwithstanding the finding made by the Inspector General in his report of May 14, 2019, the defendant
indicates in its conclusions of July 30, 2019 that it communicated to the Inspector General a register
processing activities drawn up on the basis of the model established by the DPA. The Litigation Chamber
indeed notes that the document communicated is based on the outline of the register of the activities of
processing required by Article 30 of the GDPR made available by the DPA on its website.15
Asked about the processing register – both the register required by Article 30 of the GDPR and
that required by article 6. 2 al. 4 of the Cameras Act during the hearing of March 13, 2020, the
defendant referred to its conclusions and to the document sent to the Inspector General dated
April 12, 2019 already quoted and produced in support of the canvas made available by the APD.
The Litigation Chamber notes that there is on the part of the defendant an absence of register
data processing both within the meaning of Article 30 of the GDPR and Article 6 § 2 al. 4 of the Act
Cameras and a certain misunderstanding of what such a register should contain. In this regard, no
of the particulars required by Article 30.1. of the GDPR nor by Articles 7 and 8 of the Royal Decree of 8 May
2018 relating to the declarations of installation and use of surveillance cameras and the register
15 The Data Protection Authority has indeed published on its website a model – not obligatory
– register of processing activities: https://www.autoriteprotectiondonnees.be/canevas-de-registre-des-
processing-activities

of aforementioned surveillance camera image processing activities are in fact completed.
No other data processing carried out by the defendant (such as the data of its employees

example) is listed there.

The Litigation Chamber concludes from the foregoing that the defendant does not have a register

of the processing activities it carries out – including image processing activities

by surveillance cameras – in violation of articles 30 of the GDPR and article 6. 2 al. 4 of the

Camera law.

VIII. On corrective measures and sanctions

Under the terms of Article 100 LCA, the Litigation Chamber has the power to:

1° dismiss the complaint without follow-up;

2° order the dismissal;

3° order a suspension of the pronouncement;

4° to propose a transaction;

5° issue warnings or reprimands;

6° order to comply with requests from the data subject to exercise these rights;

(7) order that the person concerned be informed of the security problem;

8° order the freezing, limitation or temporary or permanent prohibition of processing;

9° order the processing to be brought into conformity;

10° order the rectification, restriction or erasure of the data and the notification thereof

data recipients;

11° order the withdrawal of accreditation from certification bodies;

12° to issue periodic penalty payments;

13° to impose administrative fines;

14° order the suspension of cross-border data flows to another State or an organization

international;

15° forward the file to the public prosecutor's office in Brussels, who informs it of the follow-up

data on file;

16° decide on a case-by-case basis to publish its decisions on the website of the Authority for the protection of

data.

As for the lack of declaration of surveillance cameras

Compliance with transparency obligations is essential and by nature, if not

satisfied, to constitute a serious breach, more particularly when it aims to inform the

data subjects of their rights. In the present case, with regard to the absence of a statement from the cameras of

monitoring intended to make known the installation of these to the police services, the Chamber

Litigation notes that in tempore non suspecto, i.e. in April 2018, the defendant began the

declaration procedure with, at the time, the Commission for the Protection of Privacy. She

further notes that as soon as the Inspector General intervened in April 2019, the defendant notified the

cameras to the police services (May 10, 2019), thus completing the steps to put themselves in

compliance with its obligation in this regard.

Regarding the absence of a record of processing activities

As for the keeping of the register of processing activities (Article 30 of the GDPR and Article 6.2 al. 4 of the

Cameras Law), the Litigation Chamber notes that this essential accountability tool stemming from

the application of the GDPR is lacking on the part of the defendant. This lack of register since the

May 25, 2018 constitutes a serious breach since, as has been explained, this

obligation is intended to make the data controller aware of all the

processing it carries out and its obligations under the GDPR. The Litigation Chamber notes

however, as with respect to the absence of declaration referred to in the paragraph above, that

the defendant intends to collaborate with the Data Protection Authority and has, at the end of

the hearing of March 13, 2020, committed to carrying out the said register and thereby to complying.

The Litigation Chamber notes that as it is required to do so by Article 31 of the GDPR, the defendant

generally cooperated with the Data Protection Authority from the start of the Inspection

and throughout the proceedings before the Litigation Chamber.

In conclusion, in view of all the elements developed above specific to this case, the

Litigation Chamber considers that the facts found and the breach of Article 6. 2 al. 1 of the Act

cameras (absence of declaration) and articles 30.1. of the GDPR and 6. 2 para. 4 of the Cameras Law of 21

July 2007 (lack of register of processing activities) justify that, as an effective sanction,

proportionate and dissuasive as provided for in Article 83 of the GDPR, a reprimand (Article 100 § 1,

5° LCA) be pronounced against the associated defendant, with a view to bringing

compliance in the short term, an injunction to establish a register of all the activities of

processing (article 30.1. GDPR) - including its camera image processing activities

(art. 6. 2 al. 4 of the Cameras Law – that it operates and this, within a period of 3 months from the date of notification

of this decision (Article 100 § 9 LCA). In this regard, the Litigation Chamber recalls that in

application of sections 30.4. of the GDPR and 6. 2. of the Cameras Law, this register may have to be produced

ODA on first request.

Given the importance of transparency with regard to the decision-making process and the

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

data protection through the deletion of the direct identification data of the parties and

of the persons mentioned, whether natural or legal.

FOR THESE REASONS,

The Litigation Chamber of the Data Protection Authority decides, taking into account the

breaches of article 6. 2 al. 1 of the Cameras Act (absence of declaration) and Articles 30.1. from

GDPR and 6.2 para. 4 of the Cameras Law of July 21, 2007 (lack of register of processing activities),

after deliberation, to pronounce against the defendant a reprimand on the basis of article

100 § 1, 5° LCA.. This reprimand is accompanied by:

-

an injunction to establish a register of all processing activities - including

of its camera image processing activities – which it operates within 3 months to

date from the notification of this decision (article 100 § 9 LCA)

-

and an injunction to inform the Litigation Chamber of the follow-up given to the injunction

establishment of the register (above) within the same period.

Under Article 108 § 1 LCA, this decision may be appealed to the Court of

markets within 30 days of its notification, with the Authority for the protection of

given as a defendant.

Hielke Hijmans

President of the Litigation Chamber

20