1/14

Litigation Chamber

Decision on the merits 129/2021 of 26 November 2021

File number: DOS-2019-03353

Subject: Complaint for consultation of the national register by a municipal employee

The Litigation Chamber of the Data Protection Authority (hereinafter DPA), made up of Mr.

Hielke Hijmans, chairman and Messrs. Yves Poullet and Frank De Smet;

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

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

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

after GDPR;

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

Having regard to the Rules of Procedure as approved by the House of Representatives on December 20, 2018

and published in the Belgian Official Gazette on January 15, 2019;

Considering the documents in the file;

made the following decision regarding:

The complainant :

The defendant:

X, represented by Maître Gérald Horne, hereinafter “the plaintiff”;

Commune Y, represented by Maître Jean Proesmans, hereinafter the “defendant”.

Decision on the merits 129/2021 - 2/14

I. Facts and feedback

1. On May 13, 2019, the complainant sent an email to the municipality asking if everything was in order

concerning his participation in the municipal elections, given that he will be abroad at the time

elections.

2. On an undetermined date, the electoral service of the commune received postal services, the return of

the electoral summons addressed to the complainant, on which is affixed the words "does not receive/no longer
mail to the address indicated. As a result of this, the municipality decides to initiate an investigation
concerning a possible removal from domicile.

3. On May 22, 2019, the complainant was contacted by telephone by a police officer in
the framework of this investigation. The same day, the complainant contacted the municipality, informing it of his
surprised at this approach. The municipality confirms, always the same day, by return of
email that an address verification investigation is in progress.

4.

There followed an exchange of emails between the complainant and the municipality during which the latter requested
more detailed explanation of the reasons for the survey.

5.

It also appears from the complaint that the complainant is a former municipal opposition councilor in
dispute with the Mayor before the courts.

6. On June 2, 2019, the complainant contacted an official whom he believed to be the Data Protection Officer.
data from the municipality by joining the exchanges with the municipal employee and requesting a
meeting to clarify the situation amicably.

7. On June 12, 2019, the complainant sent a document entitled "GDPR complaint" to the municipality with a copy to
the Mayor. This document takes up the grievances already brought against the municipality in the
previous exchanges and indicates for the first time that the partner of the complainant's brother would have
consulted the complainant's national register in a private context.

8. On June 13, 2019, the Deputy Director General of the municipality replied to the complainant, indicating that the
person to whom the “GDPR Complaint” document was addressed is not the Data Protection Officer
data. He answers various questions from the complainant, and indicates that he suggested to the employee
municipality concerned (by
consultation of the national register) “to consider a regulation
intrafamilial”. The complainant replied to this email the same day asking for more information as to

to the identity of the data protection officer and as to the consultation of his data at the

national register.

9. On 15 June 2019, the complainant lodged his complaint with the DPA. The Front Line Service indicates

the complainant that the form must be signed. A signed complaint form is returned by the

complainant on August 15, 2019.

Decision on the merits 129/2021 - 3/14

10. This relates to irregular consultation of the complainant's national register by a member of the

communal service and on an investigation for removal of the complainant from the address at which he resides. The 3

October 2019, the complaint is declared admissible by the Frontline Service on the basis of articles

58 and 60 LCA and transmitted to the Litigation Chamber on the basis of article 62, §1 LCA.

11. On March 17, 2020, the Litigation Chamber decides to deal with the case on the merits on the basis of articles

95, §1, 1° and 98 LCA.

12. On the same day, the parties concerned are informed by registered letter of the provisions

set out in article 95, §2, as well as those of article 98 LCA. The parties are also informed

of the timetable for the exchange of conclusions on the basis of article 99 LCA.

The same letter indicates that the complaint "concerns the consultation of the personal data of the

complainant in the population registers by an employee of the municipal administration in

breach of applicable data protection rules. » Elements concerning the question of

the residence of the plaintiff and the sending of the electoral summons are therefore not examined by the

Litigation Chamber, insofar as they relate to questions of administrative law and

communal police.

With regard to the conclusions on the subject of the complaint, the deadline for receipt of the response of the

defendant is set for April 15, 2020, that of the plaintiff's reply on April 30, 2020 and finally that of

of the respondent's reply to May 15, 2020.

13. On April 9, 2020, the Defendant agrees that all communications regarding the matter will be

do it electronically.

14. On April 15, 2020, the Respondent submitted its submission in response to the Chamber
Litigation. She develops many points, some of which are not related to the framework of the
decision on the merits, as defined in point 12 and which relates specifically to the consultation of the data
from the complainant's national register. This specific point is addressed starting on page 22 of the conclusions of
the defendant, who recounts the following elements:
- That an employee of the municipality, not authorized to consult the national register, called on
another employee, empowered to consult the personal data of the complainant, and
this "for an unknown specific reason, concerning a family dispute".
- That a reprimand would have been inflicted on the employee in question and that a memorandum was
addressed to all staff regarding compliance with the applicable legislation in
regarding the protection of personal data.
-
A GDPR compliance project was already underway in the municipality in
time of the complaint. This consisted, for example, of sensitizing the agents of the municipality,

carry out an inventory of processing operations, carry out an inventory of identified risks, etc.
conclusive specifies that the non-authorized municipal employee had followed this awareness.
- That an incident such as the one described in the complaint could not happen again and that it
therefore requests a dismissal or possibly a dismissal of the complaint.
15. On April 29, 2020, the complainant sent his conclusion in reply to the Litigation Chamber. He does
also takes into account several elements that go beyond the scope of this decision on the merits (see point
12). On the question of access to the national register, he invokes the following points:
-
-
The agents are in confession and the facts are established;
The public service is responsible for the fault of its agents and the municipality is therefore

responsible for this fault;

-

Before saying right, he asks to have recourse to the Inspection Service to further instruct the

file as to the consultation listings and by questioning the two employees.

16. On May 18, 2020, the defendant indicated that it had no submissions in reply and asked to be

heard.

17. On September 28, 2021, the parties are informed that the hearing will take place on November 16, 2021.

18. On November 16, 2021, the parties are heard by the Litigation Chamber. During this

hearing, the following points were clarified:

-

It is acknowledged by both parties that a municipal employee (the plaintiff's sister-in-law)

consulted the complainant's national register, with the help of another municipal employee who

had access, for private reasons.

- The precise purpose of this consultation remains unknown. The defendant links it to a ground

inheritance, while the plaintiff considers that there is no link between these two

situations.

-

the two employees concerned (and not just one as reported in the conclusions of

the lawyer)

were reprimanded orally by the Director of Administration

municipal, after consultation with the DPO;

-

the list of logins provided by the defendant in its pleadings comes from the RN system

himself. It does not allow the traceability of the purposes of the consultation;

- A new system internal to the municipality and in the process of being put in place, which should contain

a tracking system for purposes. This should be achieved by December 15, 2021.

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

Decision on the merits 129/2021 - 5/14

II. Motivation

II.1.

Identification of the data controller

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

control of 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 8 August 1983 organizing a national register of natural persons.

21. In accordance with article 4.7 of the GDPR, it is necessary to consider as controller: “the

natural or legal person, public authority, agency or other body which alone or

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

22. In this case, the Litigation Division finds that it is indeed the defendant who determines the

purposes and means of processing. Indeed, the consultations of the National Register are carried out

only within the framework of the missions of the municipality, although the purpose of the consultations

that took place in this case is not part of these missions. Moreover, it is this which

provides the means to carry out this processing (via its computer systems). She must

therefore be considered a data controller.

23. It should also be noted that, as

reminds him

the CJEU in

his

stop

Wirtschaftsakademie of June 5, 2018, “the notion of “controller” refers to the organization

which, “alone or jointly with others” determines the purposes and means of the processing of

personal data, this concept does not necessarily refer to an organization

unique and may concern several actors (...)". That the defendant is responsible for processing

for the consultations of its employees in the National Register does not therefore mean, in this case,

that she alone corresponds to this quality. A distinction should indeed be made between consultations

National Registry within the framework of the purposes of the defendant of the abusive consultations carried out

for private purposes by a municipal employee. As shown below, although she used

the means made available to it by the defendant, insofar as the plaintiff's sister-in-law

carried out the disputed consultations outside the framework of her duties as an employee of the

defendant, it must be considered as data controller for these consultations

specifically abusive.

24. As the EDPB indicates, this nevertheless in no way exempts the defendant, as liable

processing, consultations in the National Register, its obligation to ensure the security of

treatments. This aspect is developed next. Moreover, since the complainant's sister-in-law was only targeted

by the complaint lodged with the DPA, it is not a party to these proceedings. For this reason,

the Litigation Chamber will not make any additional findings in this regard.

II.2.

Identification of processing

25. Access to the information contained in the national register constitutes processing of personal data.

personal character within the meaning of article 4.2 of the GDPR. By virtue of this qualification, this processing is

subject to the various prescriptions and obligations of the GDPR and in particular to the principles of lawfulness,

loyalty and transparency provided for in Article 5.1.a of the GDPR.

26. The principle of lawfulness indicates that any processing of personal data must have a

the bases of lawfulness listed in Article 6.1 of the GDPR.

27. It appears from the conclusions of the Respondent that it claims the basis of lawfulness of Article 6.1.e)

of the GDPR for the processing of data from the national register. This article is written as

follows:

“Clause 6

Lawfulness of processing

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

filled:

[…]

e) the processing is necessary for the performance of a task carried out in the public interest or relating to the exercise of

the official authority vested in the controller; »

According to the defendant, this mission of public interest is granted to it by the following standards:

- Law 8 of August 1983 organizing a National Register of natural persons;

- The Royal Decree of 3 April 1984 relating to the access of certain public authorities to the Register

of natural persons, as well as the updating and control of information;

- Law of 19 July 1991 relating to population registers, identity cards, cards of

foreigners and residence documents;

- The Royal Decree of 16 July 1992 relating to population registers and the register of

strangers;

- The general instructions concerning the keeping of population registers (circular of the

07/10/1992 relating to the keeping of population and foreigners registers).

Decision on the merits 129/2021 - 7/14

28. These various laws impose on municipalities certain obligations concerning the keeping and

information from the National Register and population registers. They also have access

for the exercise of their missions and are subject to certain conditions in this context. The fact for a

person to communicate information obtained from the National Register to persons not

entitled to receive them, or to make use of these data for purposes other than those for which

it has been legally authorized is criminally sanctioned1.

29. It appears from the documents in the file and the conclusions of the parties that the complainant's national register

property is the subject of unauthorized access, and that this element is recognized by the defendant itself.

same. It indicates that the unauthorized access took place on May 27, 2019 due to a consultation by a

municipal employee, assisted by a colleague, in the context of a private inheritance dispute.

30. In response to this incident, the defendant would have implemented several actions in order to avoid a

repetition of such acts. The employee in question was reportedly reprimanded and a memo

recalling compliance with applicable data protection legislation was sent to

all of its staff. The Litigation Chamber therefore considers that the facts reported by the

complainant regarding the consultation of his national register file are proven.

31. Being established in the file and acknowledged by the defendant that the data processing was carried out

for private purposes by an employee of the defendant, it cannot be considered that he enters

in the public interest mission of the defendant. The municipal employee being considered as

controller in its own right, the Chamber considers that the processing it has carried out

could constitute a violation of the principle of lawfulness established in Article 5.1.a of the GDPR. Since this

employee is not part of this procedure, the Litigation Division will not examine further

in detail its role and its compliance with the standards regulating data protection.

32.

II.3.

Reminder of the security obligation on the part of the data controller

33. Furthermore, the Litigation Division recalls that, in its capacity as data controller, the

respondent is required to implement data protection principles and must be in

able to demonstrate that these are respected (principle of responsibility – article 5.2. of the GDPR).

34. It must also, still in its capacity as data controller, implement all the

necessary measures for this purpose (Article 24 of the GDPR). The Litigation Chamber insists, as it has

already had the opportunity to recall it in previous decisions taken against agents

public2, on the fact that the public sector must, in general, be a vector of example in the

1 Law 8 of August 1983 organizing a National Register of Natural Persons, article 13.

2 See decisions 10/2019 and 11/2019 of the Litigation Chamber of November 25, 2019 pursuant to which the Litigation Chambe

recalls that the status of public representative of the controllers in question should have been accompanied by a

exemplary behavior with regard to compliance with legislation, including that relating to the protection of personal data

Decision on the merits 129/2021 - 8/14

measures it adopts to guarantee respect for the fundamental right to data protection

personal.

35. On the basis of Article 5.1.f GDPR, personal data must be processed in such a way as to

ensure appropriate security, “including protection against unauthorized or unlawful processing

and against accidental loss, destruction or damage, using technical measures

or organizational arrangements".

36. In the absence of appropriate measures to secure the personal data of individuals

concerned, the effectiveness of the fundamental rights to privacy and data protection to

personal character cannot be guaranteed, a fortiori in view of the crucial role played by the technologies of

information and communication in our society.

37. It should be noted that the principle of security' included in Article 5.1.f is now established in the GDPR

on the same level as the fundamental principles of legality, transparency and fairness.

38. The obligations of data controllers with regard to the security of processing are based on the

articles 32 et seq. of the GDPR.

39. The classic components of recommendations in terms of information security, such as

recommended by ISO27xxx are the confidentiality of data, their integrity and their

availablity. Added to these is the notion of imputability, “which makes it possible to identify, for all

the actions performed, the people, systems or processes that initiated them (identification)

and to keep track of the author and the action (traceability)”. Accountability is expressed in particular in a way

concrete by keeping a register of log files according to the principle of access logging.

40. Logging therefore consists of recording relevant information concerning the events

a computer system (access to the system or to one of its files, modification of a file,

data transfer...) in files called "log files". The information given is between

other the data consulted, the date, the type of event, the data making it possible to identify

the author of the event, as well as the reason for this access. This makes it possible in particular to identify any

consultation of abusive personal data or for a non-legitimate purpose, or even

determine the cause of an accident. Although logging is not specifically mentioned

in the GDPR, keeping a journal of log files is a technical and organizational measure

envisaged in article 32 GDPR. It constitutes a good practice, recommended to the person in charge of

processing when this measure is appropriate to the risks associated with the characteristics of the processing. .

41. The predecessor institution of the DPA (the Privacy Commission –CPVP below-) already indicated

in its Guidelines for the security of personal data information as well as

that in its Recommendations to cities and towns concerning the IT log registers that the

Decision on the merits 129/2021 - 9/14

logging is an essential element of any information security policy,

what it allows the traceability of access to computer systems3.

42. This practice has also been enshrined in the legislature, which has included this obligation in Article

17 of the law of August 8, 1983 organizing a national register of natural persons. This item is

reproduced below:

Art. 17. Each public authority, public or private body having obtained authorization to access the

information from the National Registry of Natural Persons, including police services, as well as

that those of Justice cited in Articles 5 and 8 must be able to justify the consultations

carried out, whether by an individual user or by a computer system

automatique. To this end, in order to ensure the traceability of consultations, each user keeps a

consultation register. This register shows the identification of the individual user or process

or system that accessed the data, what data was accessed, how it was

been consulted, namely for reading or for modification, the date and time of the consultation as well as

the purpose for which the data from the National Register of Natural Persons was

consulted. The register of consultations is kept for at least 10 years from the date of the

consultation. He is also certified.

The register of consultations is kept at the disposal of the Data Protection Authority.

The services of the National Register of Natural Persons also keep a register of

user consultations and communications made.

This register indicates the identification of the user who has accessed the data or obtained communication

of these, the data that have been consulted or communicated, the way in which they have been

consulted, namely for reading or for modification, or communicated, the date and time of the

consultation or communication.4

43. It appears from the conclusions of the defendant and from the hearing that such a system allowing

the recording of the purpose of the processing did not exist at the time of the disputed processing. According to

Data Protection Officer, a new system integrating this functionality would be in

development and should be operational on December 15, 2021.

44. In view of the elements set out above, the Litigation Chamber therefore concludes that there has been a violation of

Article 32 of the GDPR since the defendant did not have at the time of the facts and does not have

still do not currently have the technical and organizational measures necessary to ensure

the security of the data of the national register, in the sense that it does not have a system

allowing the logging of the purposes of the consultations. This violation is all the more

3 OPC, Recommendation No. 07/2017 of August 30, 2017.

4 Emphasis added by the Litigation Chamber.

characteristic that article 17 of the Law organizing a national register specifically imposes these

obligations, which, in this case, are not respected by the defendant.

II.4.

Link between the security obligations of data controllers and the

principles of accountability and transparency

45. As indicated above, Article 32 GDPR must be read in conjunction with Article 5.2 GDPR and Article

24 GDPR, subjecting the data controller to the principle of liability. For educational purposes,

the Litigation Chamber recalls that it is the responsibility of the controller to demonstrate his

compliance with the provisions of the GDPR, by taking technical and organizational measures

appropriate, in a transparent and traceable way, allowing in the event of an inspection to provide proof

warranties applied. The principle of accountability, read in conjunction with the principle of

transparency (article 5.1.a GDPR), allows data subjects to exercise their rights and

check the compliance of the processing carried out on their personal data. She permits

so to take responsibility.

46. Recital 63 of the GDPR adds that the right of access must be considered as a mechanism for

control: "A data subject should have the right to access personal data

that have been collected about him and to exercise this right easily and at reasonable intervals, in order to

to become aware of the processing and to verify its lawfulness."

47. These principles of accountability and transparency are articulated with Article 15 of the GDPR, which guarantees

the data subject's right of access to their personal data processed. The CPP concluded

already with regard to logging, unequivocally:

“An incomplete log file and no mention of the reason for the consultation

constitute an infringement of the useful exercise of the right of access and control available to the person

concerned. This also compromises the exercise of other rights such as the right of rectification

(article 16 of the GDPR), the right to be forgotten (article 17 of the GDPR), and the right to limit the use of

data processed unlawfully (Article 18 of the GDPR). »5

48. The Litigation Chamber recommends keeping a log file log register as a

good practice, insofar as logging is useful for any data controller, in terms of

that it makes it possible to ensure the materialization of the principle of availability, itself closely linked to the

principles of confidentiality and data integrity. The Litigation Chamber further specifies,

that it is a legal obligation enshrined in the law organizing the national register, as amended

by the Law of 25 November 2018 laying down various provisions concerning the Register

5 OPC, Recommendation no. 07/2017 of August 30, 2017, p. 10.

national and population registers which entered into force on 24 December 2018, i.e. before the disputed facts.

49. Furthermore, among the appropriate security measures intended to guarantee the confidentiality of data, a data controller such as the defendant is, according to the point of view expressed to the time by the Belgian Commission for the protection of privacy required to put in place measures organizational and technical security measures that guarantee access control6: in other words terms, only persons who, in the exercise of their own function, need access to such or such data must be able to benefit from the necessary access for this purpose.

50. The Litigation Chamber recalls in this respect Article 5.1.b of the GDPR which enshrines the principle of purpose, i.e. the requirement that the data be collected for specific, explicit and legitimate and are not further processed in a manner incompatible with those purposes. In this respect, the defendant is authorized to consult the National Register for specific purposes in accordance with the Law of 8 August 1983 organizing a National Register of natural persons.

51. The data controller must therefore ensure that the personal data are not accessible only to people and applications that have explicit permission to do so. It suits assign each person their own account and access to personal data should be be exclusively authorized by applying the need-to-know principles. These persons should only have access to the functionality or data they need for the purposes of the execution of the tasks assigned to them, in compliance with the principle of purpose.

52. It is therefore incumbent on the defendant to ensure that access to the National Registry remains limited to purposes for which this access was authorized. It is also his responsibility to be able to demonstrate. Compliance with the principle of purpose, a pillar of data protection, cannot in fact not be verified if the agents of a structure such as the defendant do not record the reason for the consultation they operate. It is equally essential in this respect that in accordance with Article 24 of the

GDPR, the defendant has an adequate control mechanism in place to ensure that its agents

authorized persons consult the National Register solely for these purposes. The defendant must

have a computer application that makes it possible to legitimize each consultation carried out by

its staff and thus demonstrates that the consultation took place within the framework of the exercise of the tasks of the

staff member who conducted the consultation.

53. The Litigation Chamber recalls that it has in the past taken decisions concerning the subject of

access to data from the national register. Thus, Decision 19/20207 requires in particular that the

data controller with access to data from the National Register sets up a control

6 See. in particular the Reference Measures in terms of security applicable to any processing of personal data enacted

by the Commission for the protection of privacy: https://www.autoriteprotectiondonnees.be/lexique/mesures-de-reference

7 Decision 19/2020 of 29 April 2020 (available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-

2020.pdf)

access, and guarantees that access to the National Register remains limited to the purposes for which

this access has been granted. It is also incumbent on him to be able to demonstrate this. These obligations

are deduced by the Litigation Chamber in particular from Articles 5.1.b and f, 5.2., 24, 32 of the GDPR and

Article 17 of the Law of August 8, 1983 organizing a National Register of natural persons.

III. Regarding corrective measures and sanctions

54. Under Article 100 LCA, the Litigation Chamber has the power to:

1° dismiss the complaint without follow-up;

2° order the dismissal;

3° order a suspension of the pronouncement;

4° 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 a

processing compliance;

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.

55. The Litigation Division points out that under Article 221.2° of the Law of 30 July 2018 relating to

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

it cannot impose a fine on the defendant, since the latter is a public authority within the meaning of

Article 5.1° of this same law.

56. The Litigation Chamber found a violation of Article 32 of the GDPR (point 44).

Decision on the merits 129/2021 - 13/14

57. In conclusion from the foregoing, and in view of all the circumstances of the case, the Chamber

Litigation considers that the reprimand (i.e. the call to order referred to in Article 58.2.b of the GDPR) is in

the case, the effective, proportionate and dissuasive sanction which is necessary with regard to the defendant8.

58. The Litigation Chamber took due note of the fact that the Respondent indicated during the

the hearing that the deployment of its new IT system should allow it to fill

the shortcomings identified by the Litigation Chamber in this decision. In order to

confirm the effectiveness of this modification implemented by the defendant, the Chamber

court orders him to send him, within four months following the adoption of this

decision, the documents demonstrating the effective implementation of a system for logging

consultations allowing in particular the recording of the purpose of the processing.

IV. Publication of the decision

59. Given the importance of transparency in the decision-making process and in view of

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

the Data Protection Authority by deleting the direct identification data

of the parties and persons cited, whether natural or legal.

8 As it has already had the opportunity to specify in several decisions, the Litigation Chamber recalls here that the warning sanc

a breach which is likely to occur: see. Article 58.2.a) of the GDPR in this respect.

FOR THESE REASONS,

The Litigation Chamber of the Data Protection Authority decides, after deliberation:

-

To impose a reprimand for violation of article 32 of the GDPR, on the basis of article

100, 5° ACL.

- To impose compliance of the processing within four months, on the basis of

of article 100, 6° LCA.

- To order the defendant to inform, with supporting documents, the Authority of

data protection (Litigation Chamber) of the continuation reserved for this

decision within the same period. This communication can be done by e-mail addressed to

the following address (contact address of the Litigation Chamber):

litigationchamber@apd-gba.be.

Pursuant to Article 108 §1 LCA, this decision may be appealed to the Court of Justice.

contracts (Brussels Court of Appeal) within 30 days of its notification, with

the Data Protection Authority as defendant.

(se). Hielke Hijmans

President of the Litigation Chamber