Litigation Chamber

Decision on the merits 62/2022 of 29 April 2022

File number: DOS-2018-03944

Subject: Sending a global email where all recipients are visible, sending

service messages without basis of legality and processing of images of a minor

without parental consent

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

Hijmans, chairman, and Messrs. Yves Poullet and Jelle Stassijns, 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

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

data protection), hereinafter "GDPR";

Considering the law of December 3, 2017 establishing the Data Protection Authority, hereinafter

"LCA";

Having regard to the internal regulations as approved by the House of Representatives on

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

Considering the documents in the file;

made the following decision regarding:

the complainant:

Madame X, hereinafter “the complainant”;

the defendant: Y, hereinafter "the defendant" or "the data controller"

Decision on the merits 62/2022 - 2/21

I. Facts and procedure

1.

On July 23, 2018, Mrs X filed a complaint with the Data Protection Authority

(hereinafter ‘APD’) against Y.

2.

The subject of the complaint concerns a group sending of data by e-mail allowing recipients to find the e-mail addresses of the other persons concerned and the sending of communications (service messages) for which the legal basis has been challenged by the complainant. Further, the plaintiff alleges that the defendant involved the minor son of the complainant to a project intended for external publication without her having been informed beforehand, a project in which photos of the son were also taken, but without having obtained parental approval from the complainant.

3.

On September 11, 2018, the complaint was declared admissible by the Front Line Service on the basis of articles 58 and 60 of the LCA and the complaint is transmitted to the Litigation Chamber under article 62, § 1 of the LCA.

4.

On October 3, 2018, the Litigation Chamber decides to request an investigation from the Service of Inspection, pursuant to articles 63, 2° and 94, 1° of the LCA.

5.

On October 3, 2018, in accordance with Article 96, § 1 of the LCA, the Chamber's request Litigation to proceed with an investigation is forwarded to the Inspection Service, as well as the complaint and the inventory of parts.

6.

On March 23, 2021, the investigation by the Inspection Service is closed, the report is attached to the file and it is transmitted by the Inspector General to the President of the Chamber Litigation (article 91, § 1 and § 2 of the LCA).

7.

The report contains findings relating to the controller and the subject of the

the complaint and concludes first of all that the data controller provides "full assistance to

youth in matters of housing" and is considered an administrative body

Flemish as referred to in article 2, 10° of the e-gov decree1 and described on the website of

the Flemish Authority2 given that the defendant meets the criteria of Article I, 3, 6°

of the Governance Decree3.

8.

The Inspection Service then notes that the complainant distinguishes between two activities of

treatment in his complaint: the alleged data leak following the communication by

e-mail of June 7, 2018, on the one hand, and the unwanted newsletters sent by e-

mail on March 27 and May 29, 2019, on the other hand.

1 Decree of 18 July 2008 relating to the electronic exchange of administrative data, M.B. of 29 October 2008.

2 https://overheid.vlaanderen.be/digitale-overheid/is-uw-organisatie-een-vlaamse-bestuursinstantie/.

3 Governance decree of December 7, 2018, M.B. of December 19, 2018.

9.

According to the Inspection Service, the first processing activity relates to the operation

and the principal mission of the defendant. The Inspection Service also considers,

on the basis of the exhibits submitted and the respondent's response, that it is sufficiently

demonstrated that the principle of transparency has been respected. The persons concerned are

sufficiently informed about the processing of their personal data in the

framework of the sending of information letters and service communications, thanks to the

information contained in the privacy statement which can be easily found on

the controller's website.

10. Furthermore, the Inspection Service notes that the defendant indicates that since

April 2018, it no longer automatically contacts the parents of young people staying at the

of Y but invites them to register via the website (opt-in system). The service

of Inspection notes that the persons concerned are invited to register themselves

to the newsletter by voluntarily indicating their e-mail address on the website

and that this registration has no blocking effect for a subsequent visit to the website.

The Inspection Service therefore concludes that the consent of the persons concerned is

sufficiently informed, specific, free and unequivocal.

11. Although the complainant does not refer in her complaint to the possibility of unsubscribing

for service communications, the Inspection Service also notes that the

data subjects still have the option of withdrawing their consent

at any time, by writing to the Data Protection Officer of the

defendant.

12. Therefore, the Inspection Service considers the first processing activity to be in compliance with the

articles 5, 6 and 4.11 juncto article 7.2 of the GDPR as well as articles 12.1, 13 and 14 of the GDPR.

13. Next, the Inspection Service finds that although the recipients of the e-mail could

take note of the identity and e-mail address of other recipients, the content

of the June 2018 communication did not contain any personal data.

14. Regarding the use of the CC field instead of the BCC field, what should be considered

as a data leak according to the complainant, the Inspection Service confirms everything

first that the defendant did not notify the incident within 72 hours to the DPA.

15. However, the Inspection Service considers that this violation of Article 33 of the GDPR must be

somewhat nuanced, in the sense that it is possible that the data controller could have

invoke the probability that the data leak will create a low risk for the rights and

freedoms of natural persons, in accordance with Article 33.1 of the GDPR, to decide on

do not notify the DPA.

16. The Inspection Service stresses in particular that the data leak was limited both in

the number of recipients (16 parents or education officials) than in the data

of a personal nature exposed (the e-mail address possibly allowing to establish
the identity of the recipients), with the consequence that the disputed e-mail has no potential
caused only very limited damage to the plaintiff.
17. The inspection report also refers to the fact that the complaint and violation
rather concerned a single unintentional and essentially human error, given the
the defendant's ICT code of conduct which indicates that employees must use
the BCC field as needed.
18. In addition, according to the Inspection Service, the data leak seems to be preventable by
the future because the defendant has learned the lessons of the situation and already has a procedure
and a form that can be used to notify a data leak.
19. Finally, the Inspection Service refers to internal awareness raising and training on
the existing ICT code of conduct and procedure for security incidents as well as the
notification form intended for this purpose that the defendant has provided since the incident
for the collaborators of the section in which the event occurred.
20. In view of the foregoing, the Inspection Service considers that the violation of
GDPR article 33.1 could be terminated. Nevertheless, the Inspection Service observes
a whole series of points of attention related to the internal procedure of the defendant.
21. The Inspection Service notes more specifically that a notification to the DPA was not
provided for in the procedure for security leaks and that the aforementioned procedure could
therefore be supplemented by specific instructions in order to always provide for a
recording of incidents in the company's own data breach register
defendant, to apologize to the persons concerned, as well as to address
subsequently to the recipients of the e-mails sent by mistake an e-mail asking them to
immediately delete the previous email.
22. As regards the second processing activity, namely the two e-mail communications from
March 27 and May 29, 2019, the Inspection Department notes that this concerns the sending of

information letters, in particular to the parents of teenagers staying in the section

of the controller.

23. The Inspection Service points out that these information letters contain a

possibility of unsubscribing listed at the bottom of the e-mails and that the persons concerned have

also the possibility of withdrawing their consent by means of a letter addressed to the

defendant's data protection officer.

24. On the basis of these specific elements present in the file, the Inspection Service

notes that the consent provided by the controller is free and unambiguous

and therefore meets the conditions set out in article 4.11 juncto article 7.3 of the GDPR. the

Inspection Service therefore does not question this processing activity on the basis of

Decision on the merits 62/2022 - 5/21

GDPR Article 6.1(a) and notes that this processing activity may be

considered to comply with Article 5.1.a) of the GDPR.

25. As to whether the Complainant was sufficiently informed of the treatment of

his personal data for the purpose of sending newsletters, the Service

Inspectorate finds that the persons concerned are adequately informed

by means of the privacy statement on the website of the controller

treatment. Consequently, the Inspection Service concludes that the sending of the letters

Disputed Information does not involve any breach of Section 12.1 and Sections 13 and 14

of the GDPR.

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

The Inspection Service notes more specifically that the register of the activities of

treatment that is presented is incomplete and imprecise and that the defendant has therefore violated

GDPR Article 30.1.

27. On September 23, 2021, the Litigation Chamber decides, pursuant to Article 95, § 1, 1° and

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

28. On February 23, 2022, the parties concerned are informed by registered letter of the
provisions as set out in article 95, § 2 as well as in article 98 of the LCA. They are
also informed, pursuant to Article 99 of the LCA, of the deadlines for transmitting their
conclusions.
29. Given that at the time when she lodged the complaint, the complainant was residing in a linguistic region
Dutch-speaking and that according to the inspection report, the defendant is considered
as a Flemish administrative body4, the Litigation Chamber also decides
to conduct the proceedings in Dutch, in accordance with its language policy5. Both
however, the parties have 14 days to object.
30. On October 6, 2021, the complainant objected to the use of Dutch as the language of the
procedure. Given the fact that when filing her complaint in French, the
complainant actually resided in the homogeneous Dutch-speaking linguistic region,
that the defendant must be considered as a Flemish administrative body and
that the complainant moreover used Dutch on several occasions in the context of her
exchanges with the defendant as well as with the services of the Agentschap
Jongerenwelzijn (Youth Welfare Agency), the Litigation Chamber decides, on
October 14, 2021, to propose to the parties the following agreement by registered mail.
4 Inspection report of March 23, 2021, p. 3.
5 Note on the language policy used by the Litigation Division, available on the DPA website via this
link
: https://www.autoriteprotectiondonnees.be/publications/note-relative-a-la-politique-linguistique-de-la-chambre-
litigation.pdf.

has. The official language of the proceedings is Dutch, it being understood that the parties
may express themselves in French or in Dutch within the framework of the procedure
before the Litigation Chamber, both in writing in their conclusions

only orally during a possible hearing.

b. The Litigation Chamber undertakes to always send to

the future its

correspondence with the parties concerned in both French and Dutch,

in accordance with article 41, § 1 and § 2 of the laws of 18 July 1966 on the employment of

languages in administrative matters (hereinafter LLC)6.

The deadlines previously communicated for rendering the conclusions will be

replaced by new deadlines.

The Litigation Chamber will also send the complainant a translation

French of the inspection report written in Dutch, without this version

French replaces the inspection report.

vs. The Litigation Chamber will not translate the procedural documents introduced by

a party for the opposing party and it will not intervene in the costs incurred

by the parties for the translation of these documents. Nor should the parties

provide translations of their pleadings themselves.

d. The Litigation Chamber undertakes to take its final decision in Dutch and

to simultaneously communicate a French version to the complainant; both

versions will be available on the APD website.

31. In the absence of objection within 7 days of the communication of the proposal

previous one, the Litigation Chamber sends the parties a new invitation to

report their findings. The deadline for receipt of submissions in response

of the defendant was set for December 6, 2021, that for the submissions in reply

of the complainant on January 3, 2022 and that for the submissions in reply of the

defendant as of January 24, 2022.

32. In accordance with Articles 95 § 2, 98 and 99 of the LCA, the parties are informed both by e-

mail only by registered mail that the scope of this case relates to violations

allegedly committed by the defendant:

1) alleged violation of articles 6 and 7 of the GDPR regarding the lack of authorization

parental responsibility for the alleged processing of images of the minor son of the complainant in

view of an external publication, without the knowledge of the complainant;

6 Laws of 18 July 1966 on the use of languages in administrative matters, M.B. of 2 August 1966.

Decision on the merits 62/2022 - 7/21

2) alleged violation of articles 5, 6 and 4, paragraph 11 juncto article 7 of the GDPR

regarding the June 7, 2018 email communication between the "[…]" section of the

defendant and the parents;

3) alleged breach of Article 12.1 and Articles 13 and 14 of the GDPR regarding

information about the newsletter in the privacy statement

of the defendant;

4) alleged violation of article 30 of the GDPR due to a register of the activities of

incomplete and inaccurate processing;

5) alleged violation of

Article 33.1 of the GDPR for procedures

internal

insufficient security leaks that provide for incidents to be

always included in a personal data leak register of the person responsible for the

processing and that incidents must, where appropriate, be notified to the DPA.

33. On October 25, 2021, the data protection officer of the defendant confirmed by

e-mail the good reception of the mail of the Litigation Chamber as well as the appendices.

34. On December 3, 2021, the Litigation Chamber receives the submissions in response from the

defendant regarding the findings relating to the subject-matter of the complaint. These findings

also include the defendant's reaction to the findings

carried out by the Inspection Service outside the framework of the complaint.

35. With regard to violation 1, the Respondent emphasizes the lack of finding on this subject by the Inspection Service and therefore considers that it is not possible for it to present a defense in this regard. For the rest, the defendant declares that its collaborators request the consent of the capable minor or of the parents if the minor is deemed not able (target age 12) to take and broadcast photos. This is also in the defendant's welcome brochure which has already been provided as part of the investigation inspection.

36. Regarding violations 2 and 3, the respondent refers to the opinion of the Inspection Service that violations were properly followed up and rectified by the manager of the treatment. The defendant also makes it known that no more similar incidents happened and therefore it is a human "rookie mistake" and unique until present, given the recent entry into force of the GDPR at the time of the incident. The defendant also emphasizes that it sets up in-house training and improvement actions regular awareness.

37. Regarding Violation 4, the Respondent states that the recommendations of the report inspection, aimed at completing the register of processing activities, have in the meantime been included in the aforementioned register. In particular, a tab with version management has been added as well as a tab on the organization and the data protection officer.

Also, a tab has been added with more explanation regarding the measurements technical and organizational as well as a tab with retention periods applied. Finally, the defendant declares that the complaint dates from 6 months after the entry into force of the GDPR and that it focused at the time on the training of its employees regarding the use of procedures.

38. Regarding violation 5, for which the Inspection Service finds that the procedure internal security incident notification system provides that the defendant notifies leaks

of data with the Vlaamse Toezichtcommissie (VTC, Control Commission

flemish), the defendant intends to rely on the information available on the website

Internet of the Flemish Authority7. The defendant then states that the persons

concerned are free to lodge a complaint with the DPA in the event of a data leak

and that it is willing to report its incidents to the DPA anyway. Finally, the

defendant confirms that the e-mails sent by mistake are now added to the

register of incidents and that employees must ask the "recipients by

error" to immediately delete the message.

39. The Litigation Division did not receive any submissions in reply from the complainant.

II. Motivation

II.1. Competence of the Data Protection Authority with regard to the proceedings

Flemish administrative

40. The Litigation Chamber first specifies, by analogy with its decision in particular

15/2020 of April 15, 20208 and as stated in the report of the Service

of Inspection, that the DPA is competent in this case to intervene.

41. The GDPR is a regulation directly applicable in the Union and cannot be

transposed into national law by the Member States. The provisions of the GDPR cannot

no longer be specified in national regulations, except as regards the points

where expressly permitted by the GDPR. Data protection is therefore in

principle which has become a subject of European law9.

42. The promulgation of any regulatory provisions relating to data to be

personal character by the federal authority or a federated authority must therefore be done in the

framework defined by the GDPR. In this regard, the Litigation Division refers to Article 22 of the

7 https://overheid.vlaanderen.be/digitale-overheid/is-uw-organisatie-een-vlaamse-bestuursinstantie.

8 Decision on the merits 15/2020 of 15 April 2020 of the Litigation Chamber of the DPA, para. 69-70 as well as 77 e.s. See

also Decision 23/2022 of February 11, 2022 and Decision 31/2022 of March 4, 2022, para. 33-43. These decisions are

available on the DPA website: https://www.autoriteprotectiondonnees.be/citoyen/publications/decisions.

9 See for example C. KUNER, L.A. BYGRAVE and C. DOCKSEY (eds.), The EU General Data Protection Regulation: A Comm

Oxford University Press, 2020, p. 54/56.

Constitution10 and to the consistent case law of the Constitutional Court on the matter which

specifies that the right to respect for private life, as guaranteed by Article 22 of the

Constitution (as well as in treaties), is broad in scope and includes in particular the

protection of personal data and personal information11.

43. The Constitutional Court and the Legislation Section of the Council of State have already ruled that

the establishment of

general limitations to the rights guaranteed by a provision

Constitutional law is a matter reserved for the federal legislator12. Therefore, the

federated authorities retain the possibility of providing, within the framework of their powers,

specific limitations, only to that extent and subject to compliance to that

regard to general federal legislation.

44. In short, the Litigation Chamber finds that the federal authority and the federated authorities

are competent to enact general and specific rules respectively

concerning the protection of private and family life, and this only concerning the points

authorized by the GDPR and in compliance with the rules of the GDPR which apply directly

in the Belgian legal order14.

45. In its opinion no. 61.267/2/AV of 27 June 2017 which was promulgated within the framework of

the preliminary draft that led to the LCA, the Legislation section of the Council of State deepened

the rules for the distribution of powers in terms of monitoring the protection of

data15. The Council of State affirmed in the aforementioned opinion that the federal authority could create

a supervisory authority with "general competence […] for all

processing of personal data, even those that take place in business

for which the communities and regions are competent”16. “Such a settlement

does not prejudice the competence of the communities and regions, […]”, according to the Council

of State17. Consequently, according to the Council of State, the supervisory authorities of the federated entities

10 “Everyone has the right to respect for his private and family life, except in the cases and under the conditions established by

rule referred to in Article 134 guarantee the protection of this right."

11 See for example Cour const., n° 29/2018, 15 March 2018, B.11; no. 104/2018, July 19, 2018, B.21; No. 153/2018,

November 8, 2018, B.9.1. See also A. ALEN and K. MUYLLE, Handboek van het Belgisch Staatsrecht, Mechelen, Kluwer, 2011

p. 917 e.s.

12 A. ALEN and K. MUYLLE, Handboek van het Belgisch Staatsrecht, Mechelen, Kluwer, 2011, 918; K. REYBROUCK and S. S

De federale bevoegdheden, Antwerpen, Intersentia, 2019, 122; J. VANDE LANOTTE, G. GOEDERTIER, Y. HAECK, J. GOOSS

T. DE PELSMAEKER, Belgisch Publiekrecht, Brugge, die Keure, 2015, p. 449.

13 Court of Arbitration, No. 50/2003, April 30, 2003, B.8.10; no. 51/2003, April 30, 2003, B.4.12; 162/2004, October 20, 2004 an

No. 16/2005, January 19, 2005; Constitutional Court, October 20, 2004, February 14, 2008; Opinion of the Council of State No.

of July 15, 2004, Doc. Speak. Speak. Fl. 2005-2006, n° 531/1: "[…] de gemeenschappen en de gewesten [zijn] slechts bevoegd

[…] om specifieke beperkingen van het recht op de eerbiediging van het privateleven toe te staan en te regelen voor zover ze

daarbij de federaal bepaalde basisnormen aanpassen of aanvullen, maar […] ze [zijn] niet bevoegd […] om die federale

basisnormen aan te tasten".

14 J. VAN PRAET, De latente staatshervorming, Brugge, die Keure, 2011, p. 249-250.

15 Opinion of the Council of State no. 61.267/2 of 27 June 2017 on a draft bill "reforming the Commission for the protection of

private life", pp. 28-45.

16 Ibid., p. 12, para. 5.

17 Ibid., p. 12, para. 6.

can only be authorized to exercise control over the specific rules that the

federated entities have promulgated for the processing of data within the framework of activities

which fall within their competence, and this of course only insofar as the GDPR

still authorizes the Member States to establish specific provisions and that it is not

not violate the provisions of the LCA.

46. In short, pursuant to Article 4 of the LCA, the DPA, as the federal supervisory authority,

is the body competent to control the general rules, the provisions of which

of the GDPR that do not require further national execution18.

This is also the case if the data processing concerns a matter which falls within the scope of the

competence of the communities or regions (federal authorities) and/or if the responsible

of the treatment is a public authority which comes under the communities or regions, even

if the federated entity has itself created a supervisory authority within the meaning of the GDPR.

47. In view of the foregoing, the Litigation Chamber concludes that in order for an authority to

control of a federated entity is competent, the fact that the data processing

concerns material of a federated entity, is far from sufficient. In addition, the federated entity

in question must also have promulgated specific rules for the treatment of

personal data in the context of this matter, within the margin left by the

GDPR to Member States. Only the control of compliance with these specific rules adopted

by the federated entities may be entrusted to the supervisory authority of the federated entity.

48. The Litigation Chamber emphasizes that the notion of “specific rules” cannot

subject to too broad an interpretation. It emerges from the cited opinion of the Council of State that the notion

of “specific rules” refers to specific limitations or particular safeguards

which derogate from or go beyond the general provisions, warranties and limitations

covered by or arising from the GDPR or federal law. In other words, the

simple fact that the federated entities implement or confirm a general rule (for

decree or order) does not mean that this rule is conferred the character of

'specific rule'. There is only a specific rule when the federated entities

establish additional safeguards or limitations using the margin left by

the GDPR for this purpose.

49. Added to this is the fact that any limitations on the powers of a data protection authority

data under the GDPR would only be possible if a supervisory authority

satisfying all requirements imposed on supervisory authorities under the Treaties

European Unions and having been entrusted with all the missions and all the powers of a

18 See also, for example, Council of State opinion no. 66.033/1/AV of 3 June 2019 on a draft government decree

of December 10, 2010 "implementing the decree relating to private placement, with regard to the establishment

of a registration obligation for sports agents", p. 5, para. 5.3; Opinion of the Council of State n° 66.277/1 of 2 July

2019 on a draft decree of the Flemish Government "laying down the procedures concerning the processing, storage and

the probative value of electronic data relating to benefits in the context of family policy", p. 7, para. 5.3.

control was created at the level of a federated entity. In this regard, reference should be made

especially in Articles 51 to 59 inclusive of the GDPR. This is not the case for the Commission of

Flemish control.

50.

It follows from the above that the Flemish administrations are subject to the

directly applicable provisions of the GDPR and that the DPA is competent in the case

to intervene. This competence also means that under Article 33.1 of the GDPR,

incidents relating to personal data, as defined in Article 4.12) of the

GDPR, must be notified, where applicable, to the competent supervisory authority,

ODA.

II.2. Lack of parental approval for taking and distributing photos of a minor

51. The Litigation Division takes note of the fact that Mrs. X complains that the defendant

reportedly had photos taken of her minor son for external publication

without her having been informed in advance or giving her permission.

52. However, the Litigation Chamber finds that the complainant replied in the negative to

the request of the Inspection Service to provide proof of this alleged processing.

The plaintiff more specifically points out that the defendant refused to

communicate more information about the project. An employee of the service of

mediation by the defendant further stated that participation in the project had

directly offered to young people, participation which could also be done by

anonymously, which is why the defendant "didn't really [ask] for

consent".

53. The Litigation Chamber notes that the defendant does not dispute that the processing

dispute took place but refers to its welcome brochure in which a declaration of

consent provides for the possibility for the head of education or for the young

'able' to give their approval for the taking and use of atmospheric photos19.

54. The Litigation Chamber emphasizes first of all that it is necessary to dissociate the protection of

personal data, covered by the GDPR, the "right to the image", which is a right of the

person provided for in Article XI.174 of the Code of Economic Law. Thus, the fact that a person

agrees to be photographed or filmed does not necessarily mean that she gives her

consent to the publication or distribution of these images. These two consents are

distinct from each other and must therefore be requested separately20.

55. The Litigation Division understands from the documents submitted in the file that the son

of the complainant was 15 years old at the time of the events. Regarding the age at which minors

19 Y welcome brochure, p. 13.

20 https://www.autoriteprotectiondonnees.be/citoyen/themes/le-droit-a-l-image/principes.

could dispose of their personal data themselves, neither the GDPR nor the law

Belgian data protection authorities do not, however, provide a definitive answer, except in

the specific context of a direct offer of information society services to

children21.

56. Although all natural persons are holders of image rights, the exercise of this

right is closely linked to the legal capacity (incapacity) of the holder22. The doctrine provides
therefore a distinction between minors with the capacity for discernment and
minors without capacity for discernment, where it should be further specified "that the
current case law evaluates
the notion of
'capacity of discernment' according to
them
concrete factual circumstances of the case and not on the basis of a specific age"23.
57. In other words, this means that in the absence of a definitive answer as to whether the
plaintiff still had parental authority over her son at the time of the court judgment
of youth and whether or not the latter has the capacity for discernment, it is
impossible for the Litigation Division to know whether the complainant's authorization was
necessary in this case for the disputed processing.
58. Consequently, it is in principle the ordinary law provisions concerning the
legal capacity (incapacity) of minors24 which apply to the exercise of their
image rights and the Litigation Chamber considers prima facie that parental approval
— as well as the consent of the persons concerned if they have the capacity to
discernment — is necessary for the processing of images of minors under 18 years of age.
59. The Litigation Chamber notes, however, that the complaint is not sufficiently substantiated
by evidence of a violation of the GDPR or data protection laws
data and that it is clearly not possible to obtain such proof25. Bedroom
Nor is contentious able to establish that the prior parental authorization
was required in this case. The Litigation Division cannot therefore, on the basis of the facts
and the legal grievances advanced in the complaint, conclude that there is a violation of
data protection regulations. In short, by virtue of the elements which
21 Article 8 GDPR; article 7 of the law of 30 July 2018 on the protection of natural persons with regard to

processing of personal data, M.B. of September 5, 2018.

22 E. GULDIX, De persoonlijkheidsrechten, de persoonlijke levenssfeer en het privateleven in hun onderling verband, Thesis of

doctorate at the Faculty of Law of the V.U.B., Brussel, 1986, p. 246-247.

23 Kh. Brussels, 24 February 1995, Ing.-Cons., 1995, p. 333, note L. MULLER; Rb. Brussels, 17 May 2002, AM, 2003, p. 138.

See also L. DIERICKX, Het recht op afbeelding, Intersentia, Antwerpen-Oxford, 2005, p. 39-42.

24 Art. 388, 488 and 1123 to 1125 inclusive of the Civil Code. Non-emancipated minors are completely legally incapacitated

general and total and are therefore represented. See also FR. SWENNEN, Het personen- enfamiliaecht, Intersentia,

Antwerpen-Cambridge, 2012, para. 265 p.s.

25 In this respect, the Litigation Chamber refers to section 3.1, A.1 of its policy of dismissal, such as

published on the DPA website: https://www.autoriteprotectiondonnees.be/publications/politique-de-classement-

without-suite-of-the-contentious-chamber.pdf.

above, the Litigation Chamber considers that no violation of the

GDPR; this complaint is therefore declared manifestly unfounded26.

60. In the event that in the present case, a publication of images of young people would have

actually took place, the Litigation Chamber wonders however to what extent

such publication of photos of minors on social media or platforms of

communication is necessary for the performance of a task in the public interest entrusted to the

defendant or is part of a legal obligation to which the defendant is

submitted. The fact that the present case concerns young people with precisely a

family situation or difficult background should, according to the Litigation Chamber, at least

less encourage caution and even lead to the non-publication of images on which

these young people are recognizable, unless parental authorization has been obtained beforehand

for specific processing purposes. Since the defendant must be considered

as a Flemish public authority27, in accordance with article 6.1 in fine of the GDPR, it

cannot in fact invoke the legitimate interest as a basis for the processing of

personal data28. In the absence of a legitimate interest or a legal obligation

for the publication of images in which young people are depicted in a

recognizable, the Litigation Chamber concludes that an authorization or, at the very least,

specific prior approval from the parents or legal guardian is required.

essential.

II.3. Lawfulness of the processing of the complainant's personal data in the context of

of the service communication of June 7, 2018

61.

It is clear that the defendant has the contact details of the parents or responsible

education so that you can communicate with them about important information

as part of its relationship with the parents of young people. The Litigation Chamber starts from

principle that there is a legal basis for obtaining this data, as referred to in

Article 6.1 of the GDPR, more specifically the necessity of the processing in order to comply with a

legal obligation (article 6.1.c) of the GDPR). For this reason, consent as

legal basis, in accordance with the conditions of Articles 4.7) and 7 of the GDPR, is not

possible for obtaining the data. The parents of young people are in fact not

free to choose whether or not to transmit their details to the defendant.

26 Same, section 3.1, A.2.

27 Investigation report of the Inspection Service, p. 3. See also para. 7 of this decision.

28 Article 6.1.f) of the GDPR: "Processing is lawful only if, and insofar as, at least one of the following conditions is

met: […] f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by

a third party, unless the interests or fundamental rights and freedoms of the data subject which require

protection of personal data, in particular when the data subject is a child. Item f) of

first paragraph does not apply to processing carried out by public authorities in the performance of their tasks."

See also para. 67 of this decision.

62. The Litigation Division verifies to what extent the defendant can share these
contact details of the complainant with third parties, in this case the parents of other young people.
In accordance with Article 5.1.b) of the GDPR, the processing of personal data
for purposes other than those for which they were initially collected cannot
be authorized only if it is compatible with the purposes for which the personal data
staff were initially collected. Taking into account the criteria listed in article 6.4 of the
GDPR and in recital 50 of the GDPR29, it should be checked whether the purpose of the processing
later, in this case the dissemination by e-mail of the complainant's contact details to
parents of other young people, is or is not compatible with the purpose of the initial processing consisting
in the collection of contact details of the complainant in the context of direct contact between
the parents of the young people and the defendant. The Litigation Chamber concludes that the
complainant provided her contact details as part of her relationship with the defendant and does not
could in no way reasonably expect the defendant to share these
same data with third parties who certainly have a specific link with the defendant, being
given that they are parents of other young people, but who are strangers to the relationship between the
plaintiff and the defendant.
63.
It follows that there is no question of compatible further processing, so that a
separate legal basis is required for the communication of the contact details of the
complaining to the parents of other young people can be qualified as lawful. A treatment of
personal data, and thus also incompatible further processing as
in the present case, is indeed lawful only if there is a legal basis to that effect. For the
incompatible further processing, Article 6.1 of the GDPR should be relied upon as well as
as on recital 50 of the GDPR. Recital 50 of the GDPR30 indicates that a basis
separate law is required for the processing of personal data for
other purposes which are not compatible with the purposes for which the data

of a personal nature were initially collected. These separate legal bases which

allow processing to be considered lawful, including processing

later incompatible, are defined in article 6.1 of the GDPR.

64. To this end, the Litigation Division examines to what extent the legal bases such as

as defined in Article 6.1 of the GDPR may be invoked by the defendant in order to

29 Recital 50 of the GDPR: "[...] In order to establish whether the purposes of further processing are compatible with those for

which the personal data was initially collected, the controller, after having

complied with all the requirements relating to the lawfulness of the initial processing, should take into account, inter alia: any link

purposes and purposes of the intended further processing; the context in which the personal data was

collected, in particular the reasonable expectations of the persons concerned, according to their relationship with the

controller, as to the subsequent use of said data; the nature of the personal data;

the consequences for data subjects of the intended further processing; and the existence of appropriate safeguards for the

both as part of the initial treatment and the planned further treatment."

30 Recital 50 of the GDPR: "The processing of personal data for purposes other than those for

which the personal data was originally collected should only be allowed if it is compatible

with the purposes for which the personal data was originally collected. In this case, none

separate legal basis from that which allowed the collection of personal data will be required. […]"

legitimize the further processing of personal data concerning the

complainant.

65. The defendant does not itself mention any legal basis enabling it to proceed

to the processing of data that is the subject of the complaint, namely the communication of the address

complainant's email to parents of other youths. Furthermore, the defendant acknowledges

explicitly that this communication was an error. The defendant does not argue

therefore not that the communication could take place nor does it attempt to justify it

by expressly invoking any legal basis.

66. On the basis of the factual elements in the file, the Litigation Division verifies

ex officio if a legal basis allowing the defendant to send the e-mail

containing the e-mail address of the complainant, visible to all recipients, may the case

appropriate be invoked, taking into account the fact that there is a simple technical means of joining

the intended recipients of the email in a single action without the email addresses being

visible to all, namely sending in BCC rather than CC.

67. Given the status of the defendant31, it cannot in principle invoke its interest

legitimate (article 6.1.f) of the GDPR) nor that of a third party for the communication of the e-mail address

of the complainant to other relatives.

68. The other legal bases listed in Article 6.1.a) to e) inclusive of the GDPR are also not

applicable in the present case given that:

▪

it does not in any way appear from the subject of the complaint or from the documents in this file that the

complainant has given consent (Article 6.1.a) of the GDPR) for the processing

in dispute, nor that the defendant intends to invoke consent;

▪

the Litigation Chamber does not consider it plausible that

disclosure of

contact details of the complainant to other parents is necessary for the execution of a

contract between the plaintiff and the defendant (article 6.1.b) of the GDPR), nor that this

disclosure would result from an obligation

legal to

which would be subject

the

defendant (Article 6.1.c) of the GDPR);

▪

there is no doubt that the disclosure of the complainant's e-mail address

was not necessary to safeguard the vital interests of the parents concerned or

of another natural person (article 6.1.d) of the GDPR) and that the communication of

contact details of the parents is necessary for the execution of a mission of interest

with which the defendant is invested (article 6.1.e) of the GDPR).

69. The Litigation Chamber considers that

the above elements demonstrate

sufficiently that the defendant cannot rely on any legal basis

31 See para. 60in fine of this decision.

attesting to the legality of the data processing as implemented by it. In addition,

the defendant does not contest the facts and asserts itself that in the e-mail in question

who is the subject of the complaint, the e-mail address of the complainant is indicated at the same time

that of the other parents in the "CC" field, rather than in the "BCC" field,

contrary to what

the ICT code of conduct provides for employees.

The defendant thus indicates that the employee who sent the communication committed

a breach of the complainant's personal data.

70. Although it appears from the documents provided by the defendant that directives

general statements were written within his organization, indicating that in emails

global, the recipients had to be placed in BCC, the complainant demonstrates that these

guidelines are not applied in practice. In the service communication of the

June 7, 2018 attached by the complainant and being the subject of the complaint, these directives were not

respected. The defendant does not deny it but affirms that it follows an error

human, presenting a unique and accidental character.

71. Despite the improvements made since then, according to the Respondent, the Chamber

Litigation concludes, by virtue of the foregoing, that the violation of Articles 5, 6
and 4.11 juncto article 7 of the GDPR has been demonstrated with respect to the service communication
of June 7, 2018, in which the contact details of all recipients remained visible.

72. As specified in the report of the Inspection Service, the Chamber
Contentious considers that, on the other hand, we cannot find a violation of Article 33.1
of the GDPR since it is not established that the data leak resulting from the
service communication of June 7, 2018 involved a risk for the rights and freedoms of
the plaintiff, and that the defendant was therefore not required to notify the breach to
of ODA.

II.4. Lawfulness of the processing of the complainant's personal data in the context of
sending newsletters to parents and education officials

73. In its reply to the Inspection Service, the defendant states that it does not consider
newsletters as direct marketing but as an essential means
to involve the parents of the young people who stay in the groups of residents, from their
provide topics of conversation in communications with their children and to
keep informed of activities such as contact with parents.

74. On the contrary, the complainant observes that electronic newsletters encourage
also the recipients to be supported, either through voluntary work or financially,
the initiatives and operation of Y, as well as the promotion of service providers
external organizations such as travel agencies.

75. Based on the information letters of March 27 and May 29, 2019 that were submitted, the
Litigation Chamber notes that the recipients concerned are invited to pay
money on a voluntary basis for the benefit of Y, which is not part of the main mission
of the defendant as a Special Youth Aid Organization. Therefore, the
Litigation Chamber considers that in this case, the newsletters are not part of

not exclusively within the framework of the Decree relating to comprehensive youth assistance but must
also be considered in part as marketing communications
direct. To this end, the Litigation Division examines what legal basis, as defined
in Article 6.1 of the GDPR, is invoked by the controller.
76. The Litigation Division understands from the response provided by the defendant to
questions from the Inspection Service32 that data subjects can register for the
electronic newsletter on its website via an opt-in. The defendant declares
also that the consents given are stored in MailChimp and that the
recipients can unsubscribe via a "reply to the newsletter" or via the button
"Unsubscribe" at the bottom of each newsletter. As part of this
investigation, the defendant was also able to ascertain that MailChimp did not record any
complainant's attempt to unsubscribe via the button provided for this purpose and that no e-mail
of the complainant did not arrive via the "reply" functionality.
77. The Litigation Chamber finds that the persons concerned are adequately
informed of the processing of their personal data for the purpose of sending letters
of information and that the defendant rightly relies on their consent as
basis for this processing. In addition, the Litigation Chamber finds that the
defendant has provided appropriate measures so that the persons concerned can
easily withdraw their consent if they wish to unsubscribe.
78. Despite the foregoing, the Litigation Chamber notes that the absence of
clear distinction between
service communications and
them
newsletters
may, however, confuse data subjects as to
on the precise basis of lawfulness. The consent of the persons concerned does not constitute

effect not an appropriate basis for communications which must be considered

as necessary for the provision of the service, such as announcements regarding

parental meetings or communications that originate from an obligation

to which the controller is subject, such as, in this case,

the involvement of parents and those responsible for education in the support service

youth33. Nevertheless, it is not for the Litigation Chamber to determine what

32 Exhibit 12, p. 1-2.

33 The Litigation Chamber refers in particular to the common commitment referred to in article 8 of the decree of July 12, 2013

relating to integral youth assistance, M.B. of September 13, 2013, applicable to the defendant:

specific legal obligation the defendant may or may not invoke as a basis

for his service communications to parents and education officials, in

as part of its main missions.

79. Following the foregoing findings, the Litigation Chamber concludes that in this case,

the defendant did not sufficiently inform the persons concerned of the distinction

between service communications and communications relating directly to its

main mission, on the one hand, and the communications which must be qualified as

direct marketing, on the other hand. In this regard, the Litigation Chamber emphasizes in particular

the importance of an appropriate legal basis for both service communications

necessary only for electronic newsletters informing parents and

responsible for education on a voluntary basis with regard to the day-to-day functioning of

the organization.

80. In the absence of clear information on the different categories of communications

information to parents and education officials, both in the

privacy statement online than in the welcome brochure, the Chamber

Litigation believes that the defendant violated Articles 12 and 13 of the GDPR.

II.5. Obligation of documentation for security incidents and obligation of notification

from the ODA

81. The Inspection Service finds in the course of its investigation that the internal procedure for

the defendant in relation to the treatment of

security incidents does not provide

explicitly a systematic recording of e-mails sent by mistake as

only incidents in the own register of data leaks and that the form intended for the

monitoring of security incidents does not everywhere provide for an obligation to notify

of ODA.

82. The Litigation Chamber recalls that a data controller must document any

violation as explained in Article 33.5 of the GDPR, whether or not the violation must be notified

to the supervisory authority:

“Integral youth care relates to cooperation and harmonization in the field of youth care with the aim

to enter into a common commitment in favor of minors, their parents and, where applicable, those responsible for

education and the people concerned in their entourage and therefore aims to:

1° to engage them with a view to the socialization of youth assistance services;

2° to organize temporary access to youth assistance services;

3° to ensure the flexibility and continuity of youth support services, including a smooth transition to other

forms of support services;

(4) to appropriately manage disturbing situations in terms of youth assistance services;

(5) to provide a subsidiary offer in youth assistance crisis services;

6° to involve them as much as possible in youth assistance services;

7° to achieve an integral approach in terms of the organization and provision of youth support services.”

Decision on the merits 62/2022 - 19/21

“The data controller shall document any data breach of a personal nature

personal data, stating the facts regarding the personal data breach

staff, its effects and the measures taken to remedy it. The documentation as well
constituted enables the supervisory authority to verify compliance with this article."
83. In the absence of a finding by the Inspection Service concerning the recording of the
data leak following the service communication of June 7, 2018 in an internal register
of the defendant's incidents, the Litigation Chamber is not in a position to conclude
that it is a violation of GDPR and data protection regulations.
data. Therefore, the Litigation Chamber decides to order the non-suit with regard to
concerns this point. The Litigation Chamber, however, takes note of the intention of the
defendant to proceed in the future with the notification of incidents via the Intranet,
notification which will be followed by an automatic e-mail to the employee concerned containing
follow-up steps, a reference to the appropriate incident management procedure and a few
examples of data leaks.
84. As for the additions that the Inspection Service proposes to include in the procedure
internal, in particular the obligation to notify breaches of personal data
personnel with the DPA, the Litigation Chamber refers to the presentation given above
concerning the general competence of the DPA for compliance with the GDPR34.
II.6. Register of processing activities
85. The Litigation Chamber concurs with the finding of the Inspection Service concerning the
incomplete and unclear nature of the record of processing activities. GDPR Article 30
explicitly provides that the register must include the name and contact details
of the controller and, where applicable, of the joint controller, of the
representative of the controller and the data protection officer.
In addition, the controller must define the deadlines for the erasure of personal data.
different categories of data, taking into account that vague deadlines such as
"unknown retention period" or "legal retention period" are not sufficient
clear. Finally, the description of the technical and organizational measures must offer the

opportunity to understand their precise effect in order to be able to verify the extent to which

personal data concerned thus benefit from effective protection.

86. Given the absence of the aforementioned information in the register of data processing activities

defendant at the time of the investigation, the Litigation Chamber considers that the violation of

Article 30 of the GDPR is sufficiently established.

34 See paras. 40-Error! Reference source not found. of this decision.

III. Publication of the decision

87. Given the importance of transparency regarding the decision-making process of the Chamber

Litigation, this decision is published on the website of the APD. However, it is not

it is not necessary for this purpose that the identification data of the parties be directly

communicated.

FOR THESE REASONS,

the Litigation Chamber of

the Data Protection Authority decides, after

deliberation:

- pursuant to Article 100, § 1, 1° of the LCA, to close the complaint without action as regards

concerns the taking and publication of the image of the minor son of the complainant, without her

has given its prior authorization;

- pursuant to Article 100, § 1, 2° of the LCA, to order the non-suit as regards

the recording of the data leak of June 7, 2018 in the internal register of

incidents;

- pursuant to Article 100, § 1, 5° of the LCA, to issue a warning with regard to the

defendant regarding the notification of personal data breaches

with the DPA, in accordance with Article 33 of the GDPR;

- pursuant to Article 100, § 1, 5° of the LCA, to issue a reprimand with regard to the defendant for infringement of Articles 5, 6 and 4.11 juncto Article 7 of the GDPR in the framework of the service communication of June 7, 2018 in which the contact details of all recipients remained visible;

- pursuant to Article 100, § 1, 5° of the LCA, to issue a reprimand with regard to the defendant for infringement of Articles 12 and 13 of the GDPR for the absence of transparency in the defendant's confidentiality statement regarding the processing grounds for service communications to parents and responsible for education on the one hand and for the newsletters to be qualified as direct marketing on the other hand;

- pursuant to Article 100, § 1, 9° of the LCA, to order the defendant to put compliance of its privacy statement with Articles 12 and 13 of the GDPR;

- pursuant to Article 100, § 1, 9° of the LCA, to order the defendant to put compliance of the record of processing activities with Article 30 of the GDPR.

Under article 108, § 1 of the LCA, this decision may be appealed in a period of thirty days, from the notification, to the Court of Markets, with the Authority of data protection as defendant.

(Sé). Hielke HIJMANS

President of the Litigation Chamber