1/32

Litigation Chamber

Decision on the merits 15/2021 of 09 February 2021

File number: DOS-2018-06125

Subject: Complaint against an SA for an unsatisfactory response to the exercise of its right of access

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

Hijmans, chairman, and Messrs. Yves Poullet and Christophe Boeraeve, members, taking over the business

in this 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 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: Mr. X, hereinafter “the complainant”.

The defendant: S.A. Y, (hereinafter “the defendant”).

1. Feedback from the procedure

1. Having regard to the complaint lodged on October 24, 2018 by the complainant with the Data Protection Authority

(ODA);

Decision on the merits 15/2021 - 2/32

2. Considering the decision of the Front Line Service to declare the complaint admissible and to transfer it to the

Litigation Chamber of September 29, 2018;

3. Given the referral to the Inspectorate by letter of November 28, 2018;

4. Having regard to the report and minutes of the Inspector General's investigation transmitted on July 9, 2019 to the

Litigation chamber;

5. Having regard to the letter dated July 25, 2019 from the Litigation Chamber informing the parties of its

decision to consider the case as ready for substantive processing on the basis of Article

98 LCA and communicating to them a timetable for the exchange of conclusions;

6. Considering the conclusions of the defendant, received on September 6, 2019;

7. Having regard to the complainant's observations sent by email and indicating that he refrains from concluding, received

October 7, 2019;

8. Having regard to the defendant's submissions in reply, received on November 5, 2019;

9. Having regard to the invitation to the hearing sent by the Litigation Chamber to the parties pursuant to

Article 46 of the DPA's Internal Rules and Article 93 of the LCA, concerning more

specifically the relationship between article 15.4 of the GDPR and recital 63 of the GDPR, as well as

balancing the right to access and obtain data with the rights and freedoms

of others;

10. Having regard to the defendant's preparatory note for the hearing of September 4, 2020;

11. Having regard to the hearing during the session of the Litigation Chamber of September 14, 2020 in the presence of

Me De Ridder, counsel for the defendant in the absence of the complainant;

2. Facts and subject of the complaint

12. The defendant is active in the computer consulting sector. The complainant incorporated

the defendant in June 2008 as an employee. He then worked as a consultant

senior. As of 2015, the complainant is regularly absent. In 2016, he was elected representative

workers.

13. In 2017, the Defendant initiated proceedings against the Plaintiff before the Court of

work, on the grounds that he would publish information on a private blog before it was returned

official by the defendant, a practice which he would refuse to put an end to despite request

of the defendant in this regard.

14. In a judgment of June 21, 2018, the Labor Court rules that the defendant cannot

dismiss the plaintiff for serious reasons, following which the plaintiff reinstated his duties within

of the defendant on June 27, 2018.

15. On July 12, 2018, the plaintiff asked his employer, the defendant, to exercise his right

access and/or copy to all personal data stored about him1. The complainant is

of the opinion that the respondent's response was unsatisfactory, following which he filed his complaint on 2

October 2018.

16. The Complainant also points out that the Respondent would take photos of the employees during

of company events and publish these photos on the company intranet, without asking

employee consent.

17. On January 18, 2019, the parties enter into a settlement agreement terminating the relationship

of work.

3. The inspection report of July 9, 2019

18. In a letter dated March 6, 2019 to the complainant, the Inspector General informed the complainant of the

following elements:

□□

his request for access and copy is not retained for the following points:

oh

its emails and IT logs because article 15, 4th paragraph of the GDPR states that the right of access

may not infringe the rights and freedoms of others, and that the copying of all its

emails and logs escape the right of access and exceed its purpose;

oh

his photos because he has access to them.

□□

his request for access and copy is retained for:

oh

the annotations in his HR file and his evaluations.

19. The Inspection Service informs the complainant that his former employer granted the request

of access and copy, and informed him that he had given him a copy of the data to which the complainant

does not have access and for which the former employer can give him a copy.

20. His request lacks precision as to whether or not the photos of staff taken were targeted.

during company events as mentioned by the complainant in his complaint.

21. Finally, the Inspector General asks the complainant to send him various documents to support

his complaint (proof of the letter requesting the exercise of his rights to the defendant,

1 See point 2.1, page 14 to 15

ensuing correspondence with the defendant, and privacy statement of the

defendant).

According to his investigation report of July 9, 2019, the Inspector General concludes in these terms:

Finding 1

The employer granted the request for access and copy, and informed him that he had given him

copy of the data to which the complainant does not have access and for which the employer can

give him a copy.

Finding 2

The complainant did not send or refer to the data protection regulations of the

workers under their employment contract (privacy policy).

On September 14, 2020, the parties are heard by the Litigation Chamber. October 12

2020, the minutes of the hearing are submitted to the parties. On October 19, 2020, the House

Litigation receives the comments of counsel for the defendant relating to the minutes,

which it decides to take up in its deliberation.

4. MOTIVATION

1. As to the procedure before the Data Protection Authority, in particular

before the Litigation Chamber

22. Pursuant to Article 4 § 1erLCA, the DPA is responsible for monitoring the principles of protection

data contained in the GDPR and other laws containing provisions relating to the

protection of the processing of personal data.

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

administrative body of the APD.2 It receives complaints that the SPL forwards to it pursuant to Article

62.1st LCA, i.e. admissible complaints when 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 on which

they relate to and come under the competence of the APD.

2 The administrative nature of the litigation before the Litigation Chamber was confirmed by the Court of

markets, jurisdiction of appeal of the decisions of the Litigation Chamber. See. in particular the judgment of June 12, 2019,

published on the APD website, as well as decision 17/2020 of the Litigation Chamber.

24. Pursuant to articles 51 and s. of the GDPR and article 4 § LCA, it is up to the Chamber

Litigation as an administrative litigation body of the DPA, to exercise effective control

the application of the GDPR and to protect the fundamental rights and freedoms of individuals

with regard to the processing and to facilitate the free flow of personal data within

within the Union.

25. As the Litigation Chamber has already had occasion to state3, data processing

are operated in multiple sectors of activity, particularly in the professional context such as

in the present case.

26. The fact remains that the competence of the DPA in general, and of the Litigation Chamber

in particular, is limited to monitoring compliance with the regulations applicable to the processing

of data, regardless of the sector of activity in which this data processing

intervene.

27. Its role is not to replace the courts of the judiciary in the exercise of the

skills that are theirs, particularly in the area of labor law.

28. Therefore, as the Respondent also points out in its pleadings4, the Chamber

Litigation is not competent to rule on the issue of compliance with the agreement

transaction between the parties, having terminated their contractual relationship.

1.1- As for the right to a fair trial and its procedural guarantees within the framework of the procedure

DPA, and more particularly before the Litigation Chamber

29. The defendant alleges a violation of the right to a fair trial and of the rights of the

defence, and in particular the principles of equality of arms, adversarial proceedings and the right to be

of course, in the proceedings before the DPA5. It develops two arguments in this regard.

30. In its submissions, the Respondent argues that it “(…) at no time was

contacted by the APD during the investigation to be heard and to be able to give its version of the facts.

The investigation therefore appears to have been carried out solely at the expense of the defendant. ODA has since

unable to take the defendant's arguments into account in its investigation. But if

3 See. decision 03/2020 of the Litigation Chamber and more generally the page the website of

the DPA dedicated to the processing of personal data of employees by their employers, available

on https://www.autoriteprotectiondonnees.be/professionnel/themes/vie-privee-sur-le-lieu-de-travail/donnees-

of-workers/data-processing-of-workers.

4 Decision 03/2020, point 3.14, p16

5 The Chamber notes that the summary submissions (of 5 November 2019) filed by Y differ slightly

of the first sets of conclusions received (of September 6, 2019) on this subject. The first set of conclusions says:

"The rights of defense and the right to a fair trial, which must be guaranteed to Y, have therefore been violated",

while the summary conclusions indicate that: "The rights of defense and the right to a fair trial,

which must be guaranteed to Y, were therefore breached in the early stages of the case” (emphasis added). This

precision is not insignificant, as will be developed below.

the defendant had been contacted as part of the investigation it could have communicated the

additional information needed by the DPA and help it shed light on this file. »

31. The second argument developed by the defendant is that the plaintiff would have

had more time to prepare its case than the defendant. This argument

will be analyzed in detail below (see “1.2.4- As to the grievance that the defendant disposed of

less time than the complainant to prepare his arguments”).

1.1.1. Place

1.1.1.1.- Regarding respect for the right to a fair trial, including the rights of the defence, before

the Litigation Chamber

32. The Litigation Chamber notes that the defendant refers to several provisions

of the GDPR concerning the right to a fair trial and its procedural guarantees.

33. Its conclusions repeat6 Article 83.87 of the GDPR as well as its recitals 1488 and 129.

34. The Litigation Division agrees with the defendant as to the importance of the application of the guarantees

procedures relating to fair trial in disputes before it. She also observes that the said

principles are applied before the Litigation Chamber. Indeed, both the principle of

contradictory, that equality of arms, and the right to be heard are scrupulously respected

before the Litigation Chamber.

35. The parties have access to all the documents in the file from the start of the disputed procedure.

(access which they are reminded of via the letter of invitation to conclude, sent on July 25, 2019 by the

Litigation Chamber to the parties), which guarantees compliance with the adversarial principle.

36. Similarly, the parties are informed of their right to be heard by the same letter of invitation

to conclude.

37. The Respondent also informed the Chamber, on its own initiative, that it did not wish to

not be heard, unless the Chamber considers it useful.9

6 points 3.1 to 3.2, pp12-13

7 “The exercise by the supervisory authority of the powers conferred on it by this article is subject to safeguards
appropriate procedural procedures in accordance with Union law and the law of the Member States, including an appeal
effective jurisdiction and due process" we underline

8 “The application of sanctions, including administrative fines, should be subject to procedural safeguards
appropriate in accordance with the general principles of Union law and the Charter, including the right to
effective judicial protection and due process. » we emphasize

9 see letter from Counsel for the Respondent dated November 13, 2019.

38. In order to compensate for a lack of information concerning certain aspects of the dispute, the Chamber
elsewhere makes application in this case of this right to convene the parties on its own initiative, when
of the hearing of September 14, 2020. The right to be heard was therefore well respected.

39. Insofar as the parties have, in the context of the disputed proceedings before the Chamber
Litigation, of an equal time to conclude and reply, that they all have access to the documents of the
file, that they can equally apply their right to be heard, it cannot
be concluded that the defendant is placed at a "distinct disadvantage" in relation to
to the complainant.10

40. The defendant cannot be followed in its argument that the principles of the
adversarial proceedings, equality of arms, and the right to be heard are not respected before the
Litigation Chamber.

41. The complaint that the proceedings before the DPA, and more specifically before the Chamber
Contentious, violates the right to a fair trial is therefore dismissed.

1.1.1.2- Additional considerations concerning respect for the right to a fair trial by the
Litigation Chamber

42. The Court of Markets has also already considered that a sufficient remedy exists in the
leader of the citizens against decisions of administrative bodies, by the possibility of introducing a
appeal before it.

43. The Court added that a lack of impartiality on the part of an administrative authority does not imply

not necessarily a breach of Article 6.1 of the European Convention on Human Rights.

Rights (hereinafter “ECHR”), if a college of law with full litigation power,

respecting itself the guarantees of article 6 .1 ECHR, can exercise control over the said

decision.

44. According to the Court, a breach of the principle of impartiality of the administration in a preliminary phase

therefore does not necessarily entail a violation of the right to a fair trial if this

violation can be corrected in a later phase.

45. The possibility of bringing an action before a body which meets the guarantees of Article 6

ECHR tends to allow such corrections12.

10 Point 3.2, p13 of the defendant's conclusions.

11 “De wetgever heeft de burger een afdoend rechtmiddel tegen de handelswijze van bestuurlijke organen (te

dezen de GBA) gegeven door precies een verhaal voor de Marktenhof te voorzien”, Hof van Beroep Brussel, sectie

Marktenhof, 19de kamer A, kamer voor marktenzaken, 2019/AR/741, 12 June 2019, p9

12 “Een gebrek aan objectieve of structurele onpartijdigheid door een administratieve overheid houdt niet

noodzakelijk een schending van artikel 6.1 EVRM in indian de beslissing van die overheid vervolgens kan worden

getoetst door een rechtscollege met volle rechtsmacht dat zelfs alle waarborgen van artikel 6.1 biedt. Een

Decision on the merits 15/2021 - 8/32

46. With specific regard to the APD Litigation Division, the Court of Markets recently

decided that:

“[…] dan nog is deze rechtsbescherming door het rechtssubject slechts wettelijk afdwingbaar voor

een rechter (die deel uitmaakt) van de rechterlijke macht [...]. De wettelijke mogelijkheid om

beroep/verhaal in te stellen bij het Marktenhof strekt er toe aan de rechtzoekende de waarborg te

verlenen van artikel 6.1 EVRM en meer in het bijzonder van het verhaal voorzien in artikel 47 HGEU

[Handvest van de grondrechten van de Europese Unie]. 13 (the Chamber's emphasis).

Free translation:

“[…] this legal protection by the data subject is only legally enforceable by a

judge (who is part of) the judiciary […]. The legal possibility of lodging an appeal before the

Court of Markets aims to offer the litigant the guarantee of article 6.1 ECHR and, more particularly,

the appeal provided for in Article 47 CEU. »

47. Consequently, in the event of a lack of impartiality by the Litigation Division, quod

not in this case, and insofar as the Market Court exercises full litigation control

on the decisions of the Chamber, it could not ipso facto be concluded that there was a breach in the

procedure to the right to a fair trial.

1.1.1.3- Additional considerations concerning the scope of the rights of defense and the principle of

contradictory

48. For all intents and purposes, two additional observations can be made regarding the scope of

rights of defense and the adversarial principle.

49. Should it be concluded that the investigation as conducted by the Inspection Service (IS) (as

DPA body exercising its functions independently of the Litigation Chamber)

should not meet the requirements of a fair trial because the IS would not have contacted a

party during the investigation, as indicated above, it should be recalled that the IS has no power

of penalty. Its role is limited to making findings and transmitting them to the Chamber.

Litigation via its report.

50. Furthermore, and primarily, while it is true that the rights of the defence, which include the right

to be heard, are part of the fundamental rights which constitute the legal order of the Union and

schending van het onpartijdigheidsbeginsel in een eerdere fase leidt bijgevolg niet noodzakelijk tot een

miskenning van het recht op een eerlijk proces indian deze schending nog kan worden rechtgezet in een latere

do. Het organizeren van een beroep dor een instantie die voldoet aan alle waarborgen van artikel 6 EVRM strekt

ertoe om dergelijke rechtzettingen mogelijk te maken”, Market Court, 2019/AR/741, 12 June 2019, p10

13 Market Court, 2 September 2020, 2020/AR/329.

are anchored in the Charter14, the fact remains that, as taught by the CJEU, the right

to be heard is not absolute and a possible restriction of this right may be possible for

a purpose of general interest. This assessment must be made in concrete terms:

“However, the Court has already considered that fundamental rights, such as respect for the rights of the

defence, do not appear to be absolute prerogatives, but may include

restrictions, provided that they actually meet objectives of general interest

pursued by the measure in question and do not constitute, with regard to the aim pursued, an intervention

disproportionate and intolerable which would undermine the very substance of the rights thus guaranteed [..].

34 . Furthermore, the existence of a violation of the rights of the defense must be assessed on the basis of the

specific circumstances of each case […].15”

Concerning more specifically the right of access to documents and respect for the principle of

contradictory, the CJEU has already indicated that:

71. Failure to provide a document does not constitute a violation of the rights of the defense

that if the undertaking concerned demonstrates, on the one hand, that the Commission relied on this document

to substantiate its complaint relating to the existence of an infringement […]and, secondly, that this complaint could not

be proven only by reference to said document]. […]

73. It is thus for the undertaking concerned to demonstrate that the result to which the Commission is

reached in its decision would have been different if had to be excluded as evidence against

an undisclosed document on which the Commission relied to incriminate this company.

74. On the other hand, with regard to the failure to provide an exculpatory document, the company

concerned need only establish that its non-disclosure may have influenced, to the detriment of this

last, the course of the procedure and the content of the Commission's decision […])” 16

51. The reasoning of the Court can be applied by analogy to the present case. The Inspection Service

is free to contact the parties or not, which it assesses independently. Furthermore, in the

case in point and as indicated above, the report of the Inspection Service is entirely favorable

to the defendant. This was therefore in no way affected by the fact that the Inspection Service

did not contact him as part of his investigation.

14 See, to this effect, CJEU, 18 July 2013, Commission and Others/Kadi, C-584/10 P, C-593/10 P and C-595/10 P, ECLI:EU:C:2013:518, points 98 and 99.

15 CJEU, 10 September 2013, C-383/13 PPU, case G. and R., ECLI:EU:C:2013:533, points 33 s.

16 ECJ, 7 January 2004, Aalborg Portland A/S et a./Commission, Aff. C-204/00, ECLI:EU:C:2004:6.

1.1.1.4 - As for the autonomy of the Litigation Chamber in relation to other DPA bodies, including the Inspection Service

52. For the sake of completeness, it should also be noted that the defendant seems confusing the role and prerogatives of the Litigation Chamber with those of other bodies of ODA.

53. As indicated above, pursuant to Article 33 § 1 LCA, the Litigation Division is the administrative litigation body of the DPA. It is not apparent from the provisions relating to the procedure before the Litigation Chamber (see article 92 to 100 LCA) that the latter would be held by the findings of the IS. Consequently, the Litigation Chamber is in no way bound by the IS findings.

54. In light of the fact that, as indicated above, in the proceedings before the Chamber Litigation the procedural guarantees linked to the right to a fair trial are respected, observation (of the Chamber's autonomy in relation to the IS) confirms the Chamber's reasoning set out above and seeking to dismiss the defendant's complaint that the procedure before the Chamber would violate the right to a fair trial.

1.1.1.5 - Concerning the legal framework surrounding the investigations carried out by the Inspection Service

55. For all practical purposes, it should also be recalled that the IS can carry out any investigation, any hearing, as well as collecting any information it deems useful17 and is not subject to a general obligation to hear, particularly in view of the fact that its intervention in the procedure consists of making findings and that he does not have the power to sanction

a part.

56. In the present case, based on the documents submitted by the complainant and not

not contacting the defendant during the investigation, the IS therefore remained within the scope of the

imposed legal requirements.

57. A similar reasoning has already been held by the Court of Markets, in a case where the plaintiff

reproached that the Litigation Chamber had decided on a schedule of conclusions, without filing

prior evidence by the parties. The Court held that no legal provision

does not impose such an obligation.

17 See Art. 72 and 76 LCA "The Inspector General and the inspectors may request in writing any information

helpful to people they deem necessary. The Inspector General and the inspectors determine the delay in

which the response to his request for information must be provided and may at any time request

additional information" (emphasis added)

58. She further added that insofar as the Complainant had the possibility of making

put forward this argument in the context of its conclusions to intervene, it could not be concluded that

illegality of the procedure before the Litigation Chamber18.

1.1.1.6- As to the grievance that the defendant had less time than the complainant

to prepare his arguments

59. The defendant also raises a disproportion between the way in which the complainant and itself

were even dealt with in the course of the investigation, in that "The DPA and [the complainant] disposed

nearly 10 months to put together their case and prepare their arguments within the framework of the

substantive treatment of this case. Whereas, conversely, the defendant learned only by

letter of July 25, 2019 that a complaint concerning the – allegedly – unsuccessful exercise of

its right of access by one of its workers was ready for substantive processing. »

60. The Litigation Chamber initiates the disputed procedure itself by sending a

invitation to the parties to conclude, following the submission by the IS of its report (in cases where such

report was requested by the Chamber or drafted on the initiative of the IS).

61. This invitation, sent to the Complainant and the Respondent on July 27, 2019, set

the deadline for concluding on the part of the defendant on September 6, 2019. The defendant

therefore had 6 weeks (and not less than a month as advanced by the conclusions by the

defendant).

62. A period of one month (October 6, 2019) was then given to the complainant to submit his

conclusions in reply, followed by a new deadline of one month for the conclusions in reply of the

defendant.

63. A period of 30 days constitutes a standard period, in particular in the administrative procedure.

Thus, the deadlines granted to the parties for the introduction of the request and between games of

conclusions before the Council of State (except administrative summary) are 30 days 19. Although

that no obligation to observe a 30-day deadline is imposed on the House – particularly

if it is not necessary - the Chamber can only note that a longer period

to this standard deadline was therefore left to the defendant to conclude. A period of 30 days has

was then left to the plaintiff to respond to the defendant, following which the latter disposed to

another 30 days for its submissions in reply.

64. As to the argument based on the fact that the letter inviting the parties (including the defendant) to conclude

does not include developments on the merits of the complaint, the Chamber recalls that the

same letter indicates to the parties the possibility of consulting the administrative file, which

18 Voy Marktenhof, 2019/AR/741, June 12, 2019, p12, published on the APD website.

19 see Royal Decree of 30 November 2006 determining the cassation procedure before the Council of State, articles

3, 13 and 14

understands the complaint. The defendant also applied this possibility as of August 1, 2019

and the entire file was made available to him on August 5, 2019.

65. The Court of Markets has also already considered that a schedule of conclusions granting one month

to the parties, and in which the defendant has the last right to conclude is in accordance with the

right of defense.

This complaint is therefore unfounded.

1.2- As to the defendant's argument that the complaint is abusive

66. The Respondent also accuses the Complainant of “misappropriating the right to

complaint”20.

67. The Respondent considers that insofar as the Complainant filed three complaints to its

against, in a period corresponding to the discussions on the financial terms of the

transaction to be made between the two parties, the plaintiff would try to put pressure on the

defendant.

68. She argues that her complaint is “manifestly abusive”21. This circumstance cannot be

retained by the Litigation Chamber, as soon as the complainant is free to access his data

personal at any time.

69. The right to lodge a complaint is guaranteed by Article 77 GDPR and forms part of the basis of the

right to data protection. By definition, the exercise by a citizen of this right cannot be

called "abusive". This grievance is dismissed.

2. As to the reasons for the decision

On the defendant's breach of its obligation to follow up on the exercise

2.1.

the complainant's right of access

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

data protection and must be able to demonstrate that these are respected. She

must also implement all the necessary measures for this purpose (principle of

liability – sections 5.2. and 24 GDPR).

20 See. Conclusions of Y p. 14 points 3.7 to 3.8

21 Ibid.

71. As a preliminary point, the Chamber recalls that the right of access is one of the major requirements of the law to data protection, it constitutes the "gateway" which allows the exercise of other rights that the GDPR confers on the person concerned, such as the right to rectification, the right of access. 22

72. Pursuant to Article 15.1 of the GDPR, the data subject has the right to obtain from the controller of processing the confirmation that personal data concerning him are or are not are not processed. When this is the case, the person concerned has the right to obtain access to the said personal data as well as a series of information listed in article 15.1 a) - h) such as the purpose of the processing of his data, the possible recipients of his data as well as information relating to the existence of his rights, including that of requesting rectification or erasure of their data or that of filing a complaint with the APD.

73. Pursuant to Article 15.3 of the GDPR, the data subject also has the right to obtain copy of the personal data which is the subject of the processing. Article 15.4 of the GDPR provides that this right to copy may not infringe the rights and freedoms of others.

74. Article 12 of the GDPR relating to the procedures for exercising their rights by data subjects provides in particular that the data controller must facilitate the exercise of his rights by the data subject (Article 12.2 of the GDPR) and provide him with information on the measures taken following his request as soon as possible and at the latest within the time limit one month from its request (article 12.3 of the GDPR). When the controller does not intend to comply with the request, he must notify his refusal within one month accompanied by the information that an appeal against this refusal may be lodged with the data protection supervisory authority (12.4 GDPR).

75. The Complainant asked the Respondent to provide him with all the personal data recorded about him, specifying that he wished to be informed of the reasons, objectives, duration of preservation etc. for each personal data stored. He also specified that his request concerned access and copying of his personal data, in this case:

□ All evaluations concerning him;□

□ Any photo on which he could be identified;□

□ Copy of his emails contained in his mailbox;□

□ Any notes, annotations, comments that are part of its resource folder□

human;□

The IT logs concerning him.□

□□

22 See in particular decision 41/2020, point 47, and more generally the fact sheet on the right of access of the□

site of□

DPA, available at https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/droits-des-□

citizens/right-of-access□

Decision on the merits 15/2021 - 14/32□

76. The Complainant also points out that the Respondent would take photos of the employees during□

of company events and publish these photos on the company intranet, without asking□

employee consent.□

77. On September 19, 2018, the Respondent sent the Complainant:□

□□

The mapping of his personal data, including in particular the purposes of□

data processing and recipients;□

The content of the personal data concerning him, processed by the defendant;□

The CVs concerning him;□

□□

□□

□ His identity photos recorded by the defendant□

78. However, on September 24, 2018, the Complainant informed the Respondent that he considered his answer□

incomplete, insofar as certain data have not been communicated to it, and puts it in□

remains to communicate these other data to him by October 1, 2018. The complainant identifies

the data he considers missing as follows:

-
-
-
-
-

emails (in which he is either the recipient or the sender)

the photos in which he is identifiable

his assessments

the IT logs concerning him

annotations or comments forming part of his HR file

79. On October 2, 2018, the defendant replied to the plaintiff that “a copy of all the data to be

personal character to which you do not have access and of which we had to give you a copy was

delivery. This point is therefore closed as far as we are concerned.

80. The defendant does not dispute that it refused to respond to the request for access as

specified by the complainant in his email of September 24, 2018.

81. The Litigation Chamber will therefore examine in the following paragraphs the conformity of

this denial of the defendant's right to data protection and privacy.

2.2 As to the obstacles invoked by the defendant to the exercise of the right of access and

copy of the complainant as specified by the latter in his letter of September 24, 2018

82. The defendant cites several obstacles to the exercise of the plaintiff's right of access, such as

specified by the latter in his letter of September 24, 2018. These obstacles are examined below.

below by category of personal data to which the complainant has requested access

and/or copy.

2.2.1- Regarding the refusal of the right of access to annotations or comments in the file

of the complainant's human resources

2.2.1.1. The point of view of the defendant

Decision on the merits 15/2021 - 15/32

83. The defendant relies in the first place on Article 15.4 GDPR, in that it considers that access

by the complainant to these data would violate the protection of the personal data of the

complainant's former line managers and human resources manager, authors

of these notes or comments. In its summary conclusions of November 5, 2019, it adds

further that:

“Furthermore, and in any event, (the defendant) confirms that the notes in question were

deleted from the HR directory. (the defendant) could therefore not be able to communicate

these notes”23.

2.2.1.2. Position of the Chamber

a- Nowak Judgment

84. To the extent that it is undisputed or undisputable that valuation notations regarding

an employee are personal data, the GDPR does apply.

85. The Litigation Chamber recalls in this regard that the notion of personal data

encompasses any type of information: private (intimate), public,

professional or commercial, objective or subjective information.

86. In the Nowak judgment,24 the CJEU clearly states that the notion of personal data

covers both data resulting from objective, verifiable and questionable elements and from

subjective data that contains an evaluation or judgment about the person

concerned.

87. This is the case for annotations for an examination which reflect the opinion or assessment of the examiner

on the individual performance of a candidate, or employee evaluation data, that

this evaluation is expressed in the form of points, a scale of values or through

other assessment parameters.25

88. Beyond the specific case of the Nowak judgment (i.e. access to an examination), the judgment concerns any advice or assessment concerning the person in question.26

b- Definition and contours of the right of access

89. The Litigation Chamber recalls that Article 15.4 of the GDPR limits the right to obtain a copy27 in the following terms: “the right to obtain a copy does not affect the rights and

23 point 4.30, p 22 summary conclusions

24 Judgment of CJEU, 20 December 2017, C-434/16, Nowak, ECLI:EU:C:2017:994.

25 Ibid, point 27.

26 Ibid, point 24.

27 Paragraph 1 of Article 15, i.e. the right of access, is not affected by this limitation.

freedoms of others. Recital 63 of the GDPR clarifies in this regard that "this right should not infringe the rights and freedoms of others, including trade secrets or property intellectual property, in particular copyright protecting the software. However, these considerations should not lead to refusal of any communication of information to the data subject (…). (emphasis added)

90. In other words, the balancing of the right to obtain a copy with the rights and freedoms of others, cannot lead to the absence of any communication of information to the person concerned.

91. In its YS v. Minister voor immigration of 17 July 2014, the CJEU28 highlights the perimeter of the right of access by referring to the protection of the fundamental right of the right to life private and de facto personal data of the data subject.

92. The Court thus specifies the right of access as being limited to personal data staff of the data subject. It does not allow access to information associated with these data. Indeed, if data appearing in documents constitutes data to be personal character (for example, surname, first name and professional e-mail address), at the

With regard to the GDPR, the document which supports it is not personal data29.

93. The CJEU thus considers that (points 57-58) “If Directive 95/46 thus imposes on the Member States

to ensure that each person concerned can obtain from the data controller

personal data the communication of all data of this type that it processes

concerning it, it leaves it to these States to determine the concrete material form that this

communication must take, as long as it is "intelligible", i.e. it allows

the person concerned to read these data and to verify that the latter

are accurate and processed in a manner consistent with this directive, so that that person can, the

where appropriate, exercise the rights conferred on it […]).

Therefore, insofar as the objective pursued by this right of access can be fully satisfied by

another form of communication, the data subject can derive neither from Article 12(a),

of Directive 95/46 or of Article 8(2) of the Charter the right to obtain a copy of the

original document or file in which this data is contained. In order not to give the person

concerned access to information other than personal data concerning him,

the latter may obtain a copy of the original document or file in which this other information

have been rendered illegible. (emphasis added).

28 CJUE, YS v Minister voor immigration, 17-7-2014, aff. attached C-141/12 and C-372/12, ECLI:EU:C:2014:2081,

para. 44

29 Legris, L., Chenaoui, H., “13. - The DPO and the right of access” in Le Data Protection Officer, Brussels, Bruylant,

2020, p. 166

94. The Litigation Division is of the opinion that, in accordance with the interpretation of the Court of Justice of

the European Union in its judgments referred to above30, that Article 15.3 does not require that a

copy of the original document is provided to the data subject.

95. Article 15.3 requires the controller to provide a copy of the personal data

personal data processed to the data subject. This right to obtain a copy of the data

does not entail the right for the data subject to obtain a copy of the original document

containing this data since in certain cases, the communication of this document could

infringe the rights and freedoms of others (see Article 15.4 mentioned above).

96. This position is also that held by the Italian Court of Cassation, in a judgment of 14

December 2018, in which the latter considers, as well as the right of access of an employee to his

assessments cannot be refused on the grounds that these assessments also contain

personal data relating to third parties31.

97. This position is also that defended by the Commission Nationale de l'Informatique

and Freedoms (CNIL) French. This is a reminder that the fact of concealing the data at

personal character concerning third parties before allowing the exercise of his right of access to the

data subject satisfies the requirement of Article 15.4 not to infringe the rights of

third32.

98. In the present case, the Litigation Division considers that the defendant's argument according to

which the right of access would infringe the data protection and privacy of former

hierarchical superiors and members of human resources who made the annotations in the

complainant's human resources file, cannot be accepted. Indeed, it was permissible to

respondent to communicate to the complainant, in response to his request, the data processed which

concern him by anonymizing the name or any personal data of the authors of such

annotations.

c- Conclusion as to the complainant's right of access to the assessments in his resource file

human

99. Insofar as the case law of the CJEU teaches that rendering data unreadable

of a personal nature concerning third parties before allowing the exercise of his right of access to the

data subject satisfies the requirement of Article 15.4 not to infringe the rights of

30 C. Docksey and H. Hijmans, The Court of Justice as Key Player in Privacy and Data Protection, European Data

Protection Law Review, 3/2019, p304.

31 Corte Suprema Di Cassazione, 14 December 2018, nr. 17153/2014, in FOCQUET, A. and DECLERCK, E.,

Gevensbescherming in de praktijk, Intersentia, Antwerpen, 2019, 93.

32 Legris, L., Chenaoui, H., “13. - The DPO and the right of access” in Le Data Protection Officer, Brussels, Bruylant,

2020, p.173

third parties, and insofar as there is no legislative provision in Belgian law aimed at limiting

the right of access of an employee to his personal data processed by his (ex) employer,33

the defendant's argument that access by the plaintiff to his data would violate the

protection of personal data of former superiors and manager

of the complainant's human resources, authors of these notes or comments, is rejected.

100. Consequently, by refusing to comply with the complainant's request for access to the annotations

contained in its human resources file, the defendant violated article 15.1 and 3

GDPR.

e- Reminder of the principle of responsibility

101. The Chamber further emphasizes that in application of the principle of liability (Articles 5.2. and

24 of the GDPR), it is up to the data controller to develop the internal procedures

intended to allow the effective exercise of their rights by the persons concerned. He him

It is also incumbent, pursuant to Article 25 of the GDPR, to integrate the necessary compliance with

GDPR rules upstream of its acts and procedures.

102. Failing this, it would suffice for a data controller to invoke copyright without further

consideration, which Article 15 of the GDPR does not allow.

103. To the extent that notes taken by an employer (or executives or members of the resources

human resources) concerning the management of employees are in the vast majority of cases data

of a personal nature, the guarantees of the GDPR must apply to them. Those data

will often focus on employee identity, training, career management, where evaluation

professional. It is therefore up to the employer, as indicated above, to develop the procedures

adequate internals.

104. These internal procedures within the framework of human resources management can be

different nature.

105. We can note the example of the “comments” areas provided for in the context of the evaluation of

employees. The information inserted therein must be objective, relevant, adequate and

not excessive. A drop-down menu or keyword filtering system can, for example,

facilitate this. Writers of annotations should also keep in mind that employees

can access information about them at any time.

106. The employer also remains, as data controller, bound by all other

GDPR obligations.

33 see infra point “b.2- The argument taken from the protection of the defendant’s business secret and the interpretation

restrictive of limitations to the right of access”)

2.2.2- Regarding the refusal of the right of access to the IT logs concerning the complainant

2.2.2.1-The obligation of security of personal data and the logging of

IT logs

a- The contours of the safety obligation

107. On the basis of Article 5, 1, f GDPR, personal data must be processed in a manner

so as to ensure appropriate security, "including protection against unauthorized processing

authorized or unlawful and against accidental loss, destruction or damage, using

appropriate technical or organizational measures”.

108. In the absence of appropriate measures to secure the personal data of

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

personal data cannot be guaranteed34, a fortiori in view of the crucial role played by the

information and communication technologies in our society.

109. It should be noted that the principles of “integrity, confidentiality35 and availability36” set out in

article 5.1, f) are now erected in the GDPR at the same level as the fundamental principles

lawfulness, transparency, loyalty.

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

GDPR Articles 32 et seq.

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

recommended by ISO27xxx37 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 actions performed, people, systems or processes that initiated them

34 The crucial role played by data security for the effective exercise of their rights by persons

concerned was enshrined in particular by the ECHR in its judgment of 17 July 2008, I. c. Finland, req. no.

20511/03, in which the Court unanimously finds a violation of Article 8 by the Finnish authorities,

on the basis of insufficient protection against unauthorized access to a nurse's medical file

seropositive. The judgment is available on the link: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-

87510%22]}

35 According to the Group 29, data integrity corresponds to “the quality by virtue of which the data are

authentic and have not been inadvertently or maliciously altered during processing, storage or

transmission. The notion of integrity can extend to computer systems and requires that the processing of

personal data on these systems remains unaltered” Group 29, WP 196, Opinion 05/2012 on Cloud

Computing, p. 18.

36Availability is understood as “the property of information, systems and processes to be accessible

and usable at the request of an authorized entity”, CPVP, “note relating to the security of personal data

staff (in Dumortier, F., Vander Geeten, V., Dargent, M., Docquir, B. and Forget, C., Knockaert, M., “

Introduction » in Legal obligations of cybersecurity and incident notifications, Brussels, Politeia, 2019,

p. 9). The concept of availability is interpreted by Working Group 29 via the "violation of availability" which

encompasses not only the accidental or unlawful destruction and loss of personal data, but

also the accidental or unauthorized loss of access to them, access being an intrinsic aspect of the

data availability. (emphasis added)

37 The ISO27xxx suite of standards is one of the main international information security standards

Decision on the merits 15/2021 - 20/32

(identification) and to keep track of the perpetrator and the action (traceability)"38. Accountability

is expressed in particular in a concrete way by keeping a register of log files according to the principle

access logging.

112. Logging therefore consists of the recording of relevant information concerning the

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

of a file, data transfer, etc. in files called "log files". Information

occasions are, among other things, the data consulted, the date, the type of event, the data

identifying the author of the event, as well as the reason for this access. This allows

in particular to identify any consultation of abusive personal data or for a purpose

not legitimate, or to determine the origin of an accident.

113. Although logging is not expressly mentioned in the GDPR39, the keeping of a

journal of log files constitutes a technical and organizational measure envisaged in the article

32 GDPR. It constitutes a good practice, recommended to any data controller. Those

measures must be adapted to the risks.

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

already in its Guidelines for the security of personal data information

personnel40 as well as in its Recommendations41 to towns and municipalities42 concerning

38 Dumortier, F., "Chapter 4 - Cybersecurity, privacy, accountability, logging and log files" in Les obligations

legal cybersecurity and incident notification, Brussels, Politeia, 2019, p. 187 and APD, "Note on

personal data security, p2

39 Conversely, Directive (EU) 2016/680 attaches particular importance to the consultation and disclosure

(the most common treatment). and imposes the identification of the author of the treatment as well as that of the recipients

in the event of disclosure, the exact moment, as well as the justification of the processing (of April 27, 2016 relating to the

protection of natural persons with regard to the processing of personal data by the authorities

authorities for the purposes of the prevention, detection, investigation and prosecution of criminal offences.

matters or the execution of criminal penalties, and on the free movement of such data)

40 Available on the link https://www.autoriteprotectiondonnees.be/publications/lignes-directrices-pour-la-

information-security.pdf.

41 Recommendation to towns and municipalities concerning the recording of the reason for consulting the Register

by their staff members (CO-AR-2017-013), August 30, 2017, p7

42 In its recommendation to towns and municipalities concerning logging, the CPP emphasizes the importance

of logging as an "essential element of any information security policy" and indicates:

“21. The development of an adequate information security policy is necessary in order to take

measures which exclude any unauthorized access, and this in a documented manner allowing the municipality

to assume its responsibility. In its benchmark security measures applicable to any processing

of personal data, the Commission has already stressed that the establishment of a selective mechanism

research and logging is an essential element of any security policy for

information. (…) these guidelines prescribe that all access to the computer system must be traceable in order to

to verify who had access, when, to what and for what reason.

(…)

23. Finally, the Commission itself has already indicated on several occasions that recording the reason for the

consultation of the National Register is of crucial importance. In its recommendations on the management

access and users in the public sector and to the communication of information contained in the

population registers, the Commission stresses the importance of full tracing (who, what, when, why)

implying a logging of each consultation of the population registers, so that any

consultation of data for a non-legitimate purpose or for personal purposes can be detected and sanctioned.

Decision on the merits 15/2021 - 21/32

IT log registers that logging is an essential element of any policy

information security, in that it allows the traceability of access to systems

computers43.

b-Link between the security obligations of data controllers and the principles of

accountability and transparency

115. The Chamber recalls that 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. He

it is the responsibility of the data controller to demonstrate compliance with the provisions of the GDPR, by

taking appropriate technical and organizational measures, in a transparent and

traceable, allowing in the event of an inspection to provide proof of the guarantees applied.

116. 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 monitor the compliance of

processing carried out on their personal data. It thus makes it possible to assume the

responsibility44.

117. Recital 63 of the GDPR further adds to this that this right of access must be considered as

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

personal data that have been collected about him and to exercise this right easily and at

reasonable intervals, in order to become aware of the processing and to verify its lawfulness."

118. 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

already concluded with regard to journaling, 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). (p10) (emphasis added)45

119. The Litigation Chamber recommends the keeping of a log file log register as a

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

By extension, this obligation is also valid for consulting and updating the National Register. » (p8)

(the Chamber underlines)

43 Although this recommendation is addressed to municipalities and towns, the reasoning applies to other types

data processing, especially when it comes to sensitive data.

44 See recital 78 GDPR.

45 Along the same lines, see decision of the Sectoral Committee of the National Register of 11/01/2012.

Decision on the merits 15/2021 - 22/32

in 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.

120. As indicated above, the effectiveness of the fundamental rights to privacy and to the protection of

personal data depends significantly on the measures put in place to ensure

the security of these46, keeping a register of logs is therefore strongly recommended by the

Litigation Chamber, in view of the good practices followed by many companies.

2.2.2.2 Regarding the defendant's refusal to respond to the complainant's request for access

to its IT logs

121. With regard to the plaintiff's request for access to the IT logs concerning him, the defendant justifies

its refusal by two arguments. It emphasizes, in a first argument, (like access to

annotations in the complainant's HR file) the right to privacy of the authors of the IT logs such as

reason for refusing the complainant's right of access to the IT logs concerning him.

122. In view of the case law of the CJEU according to which rendering data unreadable to

personal character concerning third parties before allowing the exercise of his right of access to the

data subject meets the requirement of Article 15.4 GDPR not to infringe the rights

third parties, and insofar as there is no legislative provision in Belgian law aimed at

limit an employee's right of access to their personal data processed by their (ex) employer,

the defendant's argument that the plaintiff's access to the IT logs concerning him

would violate the protection of the personal data of the authors of these logs is rejected.47

123. The defendant advances as a second argument to refuse to grant the request

access to all IT logs about the complainant the amount of work

disproportionate that it would ask the defendant, linked to the enormous amount of logs and

information to verify for this purpose.

124. The CJEU ruled in its Rijkeboer judgment on the balance to be struck between the right of access of

data subjects and the extent of the burden that the obligation to satisfy this right imposes

for the controller. More specifically, the questions were to know from

when “the exercise of the right of access to information concerning the past can legitimately be

paralyzed by erasing this information. And for how long do people

holding data are required to keep records of past actions performed on these

data”48.

46Dumortier, F., Vander Geeten, V., Dargent, M., Docquir, B. and Forget, C., Knockaert, M., “Introduction” in Les

legal cybersecurity and incident notification obligations, Brussels, Politeia, 2019, p. 9 p 141

47 See point 2.2.1.2. c), page 24.

48 C. de Terwagne, “The extent over time of the right of access to information on data recipients

of a personal nature”, note under C.J.U.E., December 22, 2010, R.D.T.I., n° 43, 2011, p. 73 in Tombal, T., “

125. Although in this case the question raised was that of the time that a data controller

must keep the personal data, the reasoning of the Court can be transposed to the case

in this case, given the scope of the plaintiff's request, extending to all IT logs on

regarding. The Litigation Chamber emphasizes, in particular, the importance of finding “[..] a

fair balance between, on the one hand, the interest of the data subject to protect his private life,

in particular by means of the means of intervention and appeal provided for by the directive and, on the other hand

part, the burden that the obligation to keep this information represents for the person responsible for the

processing ".

126. The parameters founding this balance must, of course, take care not to impose

disproportionate obligations and excessive burdens, to the controller.

127. In the present case, the defendant emphasizes the disproportionate workload that would represent
a systematic search of all the IT logs concerning the complainant, since he took office
in June 2008, until the termination of his employment contract with the defendant in 2019. The
Furthermore, the complainant did not provide any explanation as to his interest in this request. He has not
did not submit conclusions and did not return to this point in his email sent to the Chamber
Litigation after submission of its conclusions by the defendant. The Litigation Chamber
cannot therefore perceive any specific need justifying the heavy workload that
would represent the systematic search linked to the request for access to all the IT logs on
concerning by the complainant.

128. In these circumstances, the Litigation Division follows the defendant in its reasoning
that granting the complainant's request would impose an obligation on him
disproportionate to the complainant's interest in exercising his right to data protection. There is
therefore no violation on the part of the defendant of the right of access to the IT logs
regarding the complainant.

2.2.3- Regarding the refusal of the right of access to the complainant's evaluations

129. The complainant also requested access to and a copy of his assessments. The defendant informs
this regard only insofar as the complainant was regularly absent from October 2015
(he worked less than 30 days in 2016, less than half of the year in 2017, about thirty
days in 2018 and no days in 2019), there was no operational evaluation or maintenance
since 2013. The defendant therefore had no personal data to communicate to the
complainant in this regard.

Section 2. – Right of access (article 15 GDPR)" in General Data Protection Regulation (RGPD/GDPR),
Brussels, Editions Larcier, 2018, p. 432-447.

130. In these circumstances, and insofar as the defendant cannot be criticized for not

not grant a request for access and copy of personal data that does not exist, the grievance
of the complainant is dismissed.

2.2.4- As for the refusal to request a copy of emails

131. In its conclusions, the defendant justifies its refusal to grant the request for a copy of the
emails (the complainant had access to the emails in question at the time of his request) in which
the complainant is the recipient or sender on the basis of article 15.4 GDPR, being the right to life
privacy of the other recipients or senders concerned by the emails in question. In his
written observations for the hearing of September 14, 2020, the defendant raises
additional arguments.

132. She first pointed out that the complainant had access to all these emails when he
request. It then highlights the right to privacy of other senders or recipients
emails, as well as that of the defendant as a legal entity, i.e. its right to
trade secret protection. Finally, the defendant notes the secrecy of the
electronic correspondence attached to the emails concerned.

The fact that the complainant had access to the emails does not prejudice his right to obtain a copy

133. The defendant raises its main argument to refuse to grant the request for a copy of the
complainant of the emails (in which he is sender or recipient) the fact that the complainant was
access (at the time of his request).

134. However, the Chamber notes that, as indicated in his complaint, the Complainant took care to explain
for what reason it specifically requests the copy of the emails. He thus explains that for
confidentiality reasons (the defendant's security and privacy policy prohibits this
formally) and technical (emails being stored on a cloud system and not on
the complainant's computer), although he had access to these emails from his professional computer,
it is impossible for him to take a copy of it.

135. Although in the present case it appears from reading the complaint that the complainant did not request access
to its emails, but only to a copy thereof, the Chamber recalls, for all practical purposes,

that the fact that a complainant is aware of the personal data about him being processed

by the data controller does not constitute a valid reason for the latter to refuse

access.

136. Indeed, no exception comparable to that provided for in Article 13.4 of the GDPR (absence

information obligation when and insofar as the data subject already has

Decision on the merits 15/2021 - 25/32

information) or Article 14.5 a) of the GDPR (absence of information to be provided in the event of

indirect collection when the data subject already has this information) does not exist

GDPR Article 15. The right of access enables the data subject to ensure that no

data concerning him is not processed without his knowledge and constitutes a first step towards the exercise

possible rights of rectification, erasure or objection. The purpose of the right of access is

therefore well beyond the mere knowledge of the data processed, which is why the

the fact that the data processed would be known to the data subject is irrelevant.

137. Respondent's argument to refuse the request for a copy, on the basis of the fact that the

complainant had access to the emails in question is irrelevant and therefore cannot be tracked.

The privacy rights of other senders or recipients in those emails

138. The defendant invokes, in order to refuse to comply with the request for a copy of the emails, the right to

the privacy of other senders or recipients in these emails, on the basis of article 15.4

GDPR.

139. The Chamber refers to the reasoning regarding the notations in the files of the

complainant's human resources49.

140. Thus, given that the case law of the CJEU teaches that making documents illegible

personal data concerning third parties before allowing the exercise of his right

of access50 to the data subject satisfies the requirement of article 15.4 GDPR not to carry

infringement of the rights of third parties, and insofar as there is no provision in Belgian law

legislation to limit an employee's right to access and copy their personal data

processed by his (ex) employer, the defendant's argument that access by the complainant

to the emails of which he is the sender or recipient and that the granting of copies of the emails would violate

the protection of personal data of other recipients or senders of emails

in question is rejected.

The protection of the defendant's trade secret and the restrictive interpretation of the limitations on the

permission to access

141. As a preliminary point, the Chamber recalls that the right of access (which necessarily covers the right to

copy, insofar as it is a prerequisite) is one of the foundations of the right to data protection,

it constitutes the "gateway" which allows the exercise of the other rights that the GDPR confers on the

concerned person. To this extent, according to consistent case law of the Court of

49 See point 2.2.1.2.c - page 24

50 It should be specified that the right to copy being intrinsically linked to the right of access and necessarily

preceded by it, this reasoning applies equally to the right of access and the right to copy.

Justice51 52, as well as as indicated in the guidelines of the EDPB53, any derogation from the

right to data protection and privacy must be interpreted restrictively. A

limitation to the right of access, should it arise, should therefore be

interpreted restrictively.

142. With regard to these limitations, the CJEU recalled in its Nowak judgment that “(…) Member States

may take legislative measures to limit the scope of the obligations and rights

provided for, in particular, in Article 6(1) and Article 12 of that directive, where such

limitation constitutes a necessary measure to safeguard the rights and freedoms of others. (period

60).

Article 23.1 GDPR states:

“Union law or the law of the Member State to which the controller or the data processor

is subject to may, by means of legislative measures, limit the scope of the obligations and

rights provided for in Articles 12 to 22 and in Article 34, as well as in Article 5 insofar as the provisions
of the right in question correspond to the rights and obligations provided for in Articles 12 to 22, when a
such limitation respects the essence of the fundamental rights and freedoms and that it constitutes a measure
necessary and proportionate in a democratic society to ensure [an important objective
of general public interest]"
143. This provision should be read in conjunction with Section 52 of the Bill of Rights
Fundamentals of the European Union and Article 8 of the European Convention on Human Rights
Rights, governs the limitation of the rights of the data subject.
144. The CJEU indicates that such a limitation of a fundamental right must be provided for by law, respect
the essential content of those rights and, in application of the principle of proportionality, be
necessary and effectively meet objectives of general interest recognized by the Union (…)"
and recalls that "derogations and limitations to these rights must operate within the limits of the
strictly necessary"54.
51 In its judgment of 11 December 2014, Ryneš (C-212/13, EU:C:2014:2428), the Court of Justice thus indicates
that "the protection of the fundamental right to privacy, guaranteed by article 7 of the charter, requires that
derogations from the protection of personal data and the limitations thereof take place in the
limits of what is strictly necessary. Insofar as the provisions of Directive 95/46/EC, in so far as they govern
the processing of personal data likely to infringe fundamental freedoms and, in
particular, to the right to privacy, must necessarily be interpreted in the light of the fundamental rights
which are included in that charter, the derogation provided for in the second indent of Article 3(2) of that directive
must be interpreted strictly" (points 27-29)
52 See also judgment of 6 October 2015 (Grand Chamber), Schrems (C-362/14, EU:C:2015:650), paragraph 92
53 Guidelines 10/2020 on restrictions under Article 23 GDPR, available at https://edpb.europa.eu/our-work-
tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en
54 Judgment of 9 November 2010 (Grand Chamber), Volker und Markus Schecke and Eifert (C-92/09 and C-93/09,
EU:C:2010:662), paragraph 65 and judgment of 27 September 2017, Peter Puskar, (ECLI:EU:C:2017:725) paragraph 116

145. Group 29 clarifies regarding the condition that the limitation be provided for by law (requirement of legality) that any interference with a fundamental right such as the right to the protection of personal data must be provided for by a law formulated in clear, precise terms and accessible, and whose effects are foreseeable for the data subject.

146. Regarding the processing of personal data in the context of employment relations, Article 88 GDPR provides that “Member States may provide, by law or by means of agreements collective rights, more specific rules to ensure the protection of rights and freedoms with regard to concerns the processing of personal data of employees in the context of professional relationships (…) ". However, such provisions do not exist, to our knowledge.

147. The Chamber notes that there is no legislative provision in Belgium aimed at limiting the right of access of an employee to his personal data processed by his (ex) employer.

148. Consequently, in view of the developments above, insofar as business secrecy tends to limit the fundamental right to data protection, it must be interpreted in such a way restrictive. Nevertheless, the Litigation Division is of the opinion that it is appropriate to carry out an analysis on a case-by-case basis, in particular when the risk to business secrecy is sufficiently demonstrated.

149. It is also worth recalling the requirement of recital 63 of the GDPR, according to which the right access "should not infringe the rights or freedoms of others, including the secrecy of business or intellectual property, including copyright protecting software. However, these considerations should not result in refusing any communication information to the data subject. (emphasis added)

150. The Chamber also notes that Directive 2016/943 on trade secrets55 emphasizes in its recitals 34 and 35 the importance given to respecting the right to data protection, in in particular the right of access, which the trade secret should not infringe:

“(34) This Directive respects the fundamental rights and observes the principles recognized

in particular by the Charter, in particular the right to respect for private and family life, the right to

protection of personal data, freedom of expression and information, freedom

occupation and the right to work, freedom of enterprise, the right to property, the right to good

administration, and in particular access to files, while respecting business secrecy, the right

to an effective remedy and to have access to an impartial tribunal and the rights of the defence.

55 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of know-how

and undisclosed business information (trade secrets) against obtaining, using and disclosing

illicit (Text with EEA relevance)

(35) It is important that the right to respect for private and family life and the right to

protection of the personal data of any person whose personal data

personnel may be dealt with by the holder of a trade secret when taking action

intended to protect a trade secret, or of any person concerned by legal proceedings

relating to the unlawful acquisition, use or disclosure of trade secrets covered by this

Directive, and whose personal data are being processed. Directive 95/46/EC

of the European Parliament and of the Council (10) governs the processing of personal data

carried out in the Member States within the framework of this Directive and under the supervision of the authorities

authorities of the Member States, in particular the public independent authorities designated by

member states. Therefore, this Directive should not affect the rights

and obligations set out in Directive 95/46/EC, in particular the data subject's right to access

to the personal data concerning him which are the subject of processing and the right to obtain

the rectification, erasure or blocking of this data when it is incomplete or

inaccurate and, where applicable, the obligation to process sensitive data in accordance with Article 8,

paragraph 5 of Directive 95/46/EC. (emphasis added)

151. The Litigation Chamber also refers to the reasoning of Working Group 29 as to the

right to data portability (article 20 GDPR), the exercise of which may not affect the

rights and freedoms of others (article 20.4 GDPR), like the right of access and copy (article 15.4 GDPR). The wording of this limitation in both articles is identical. In this measurement, and taking into account the fact that both the right of access and copy, and the right to data portability are among the fundamental components of the GDPR, the Chamber is of the opinion that the reasoning of Group 29 regarding limitation can also be applied to the right of access and copy.

152. Group 29 specifies with regard to the limitation of the right to portability by trade secrecy that a "potential risk to business cannot, however, on its own, serve as a basis for justifying the refusal to comply with a portability request"56. The risk for secrecy business must therefore be clearly demonstrated by the controller. In the case case, although this was not developed in the written documents of the defendant, the Counsel for the latter explained during the hearing that because of his position as a manager, the complainant knowledge of the identity of the defendant's customers, the amounts of the orders and the invoices to these customers, which constitute potentially sensitive business information of the defendant. The defendant also indicated that the plaintiff published on a private blog information that is still confidential, before management publishes it through official channels (facts partially or entirely at the origin of the dispute before the Labor Court between itself and the complainant). The Chamber also takes note of the complainant's request for a copy of all the emails in which he is the recipient or sender.

56 Group 29, Guidelines on the right to data portability, WP 242, 13 April 2017, p. 12

153. As indicated above, although trade secrets should be interpreted restrictively when this constitutes a limitation to the fundamental right of data protection, in In this case, the Litigation Division considers that, given the information potentially sensitive contained in the emails in question the risk for the business secrecy of the defendant is sufficiently demonstrated.

154. The Chamber is therefore of the view that the Respondent did not violate Article 15.1 and 3 by refusing to

follow up on the complainant's request for a copy of the emails in which he is the recipient or

shippers.

155. For all practical purposes, the Chamber adds that in cases where the risk is not demonstrated, it is appropriate

to apply the teaching of the case law of the CJEU (see above), according to which the fact of

make personal data concerning third parties illegible before allowing the exercise

of his right of access to the data subject satisfies the requirement of Article 15.4 not to carry

infringement of the rights of third parties.

c- The argument taken from the secrecy of the electronic correspondence of the other recipients or

senders of the emails concerned

156. The defendant then raises Article 124 of the law of 13 June 2005 relating to communications

electronic documents, as a last argument to justify its refusal to grant the request for access

and copies of the plaintiff's emails in which he is the recipient or sender.

157. However, this provision only applies to third parties to electronic communications

concerned, and not to a person party to the communications, as clearly indicated by

the Court of Cassation in a judgment of 22 April 201557.

This argument is not convincing, and is therefore dismissed.

d-Conclusion as to the defendant's refusal to comply with the request for a copy of the emails of the

plaintiff

158. The arguments of the defendant to justify the refusal to comply with the request for a copy

of the emails in question taken from the right to privacy of the other recipients or senders of the

emails, as well as the secrecy of electronic correspondence do not convince, and are therefore

discarded. However, in the present case, the argument based on the defendant's business secrecy

is relevant. There is therefore no breach of Article 15.3 of the GDPR.

2.2.5- As for the refusal of the right to copy the photos on which the complainant is

identifiable

159. In this part of his complaint, the complainant clarifies that he is not invoking the violation of the right of access

or copy, but his image rights. He indicates that photos of the employees were taken during

57 Cass. (2nd ch.), April 22, 2015, J.T., 2015, p. 1021 and 1022

Decision on the merits 15/2021 - 30/32

events of the company, without their consent, and that they are disseminated (on the intranet of

defendant company) without consent.

160. In a letter dated 6 March 2019, the DPA Inspection Service informed the complainant that his

complaint lacks clarity regarding whether or not the photos of the members of the

staff at company events, and asks them for more details on this subject.

161. However, while the taking and dissemination of targeted photos requires a legal basis, this is not the case for

untargeted photos (in which staff members cannot be identified)

clearly). In an email of June 8, the complainant specifies that during the events of the photos

portraits are taken, and that for these a prior consent is not requested nor for

taking photos or for distribution.

162. The Litigation Chamber notes that the defendant invites its employees who do not wish

that the photos in which they appear are recorded or disseminated on the intranet at

contact the DPR (Data Protection Representative) to notify him and undertakes that these

any photos are erased.58

163. The complainant did not provide any proof of the existence and/or distribution of targeted photo(s)

of him, and does not indicate that such photos or portraits of him would have been taken during events

business organized by the defendant.

To this extent, the Chamber notes the absence of violation of the complainant's image rights.

5. Corrective measures and sanctions

164. Based on the above analysis, the Litigation Chamber considers that by refusing to follow up on the

Complainant's right of access and/or copy of annotations in their resource file

human beings, the data controller has breached Articles 15.1 and 15.3 of the GDPR

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;

58 Analysis of Exhibit 37 submitted by the defendant (an email sent to all staff members

on 04/10/2018).

Decision on the merits 15/2021 - 31/32

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.

It is important to contextualize the breach of Articles 15.1 and 15.3 of the GDPR on the other hand in view

to identify the most appropriate sanctions and/or corrective measures.

165. As indicated above, the right of access (Article 15.1) is one of the foundations of the GDPR. As to

breach of the right to copy (article 15.3), the Litigation Chamber notes that obtaining

of a copy of the data is the major contribution of the GDPR in terms of the right of access. She must

allow the strengthening of the control of the persons concerned over the personal data

concerning them. The informational self-determination of which the GDPR is marked finds in this

new version of the right of access (including the right to obtain a copy) one of its most

strong expressions.

166. By refusing to communicate data concerning him to the plaintiff, the defendant deprived

the complainant of the right conferred on him by Article 15 of the GDPR but more broadly, it has infringed

to its informational autonomy by not allowing it to become acquainted with these

data.

167. Nevertheless, an order to follow up on the request for access to the annotations in the HR file

concerning the plaintiff cannot be issued, insofar as the defendant erased these

annotations after the complainant's request. In this regard, the Chamber orders the Respondent

to provide him with a sworn statement attesting to the fact that these annotations have been

erased after the plaintiff's request via the address litigationchamber@apd-gba.be within a

30 days from the notification of this decision.

168. The Litigation Chamber also takes note of the fact that the defendant is a company

of medium size, occupying 40 to 50 employees, and that it has never previously been subject to

ODA sanctions.

169. The Chamber also notes that the Respondent reacted and complied with the Complainant's requests,

some of which cover a wide range of data, albeit incompletely.

170. The efforts raised in the defendant's conclusions in terms of information security

and data protection are also taken into account. Therefore, the Litigation Chamber decides

not to impose a fine or reprimand.

171. Considering 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 Data Protection Authority by deleting the direct identification data

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

FOR THESE REASONS,

THE LITIGATION CHAMBER

Decides, after deliberation:

- To order the defendant to communicate to the Litigation Division a statement on

the honor attesting to the fact that the annotations in the human resources file relating to the

complainant were deleted after his request for access, via the address litigationchamber@apd-gba.be

within 30 days of notification of this decision;

- To order the defendant to bring the processing into conformity with regard to the annotations in the

within the human resources files of its staff, in accordance with Article 15 GDPR.

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