Decision of the National Commission sitting in restricted formation on

the outcome of inquiry No. […] conducted with Administration A

Deliberation no. 23FR/2021 of June 29, 2021

The National Commission for Data Protection sitting in restricted formation,

composed of Mrs. Tine A. Larsen, president, and Messrs. Thierry Lallemang and Marc

Lemmer, commissioners;

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

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

personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Having regard to the law of August 1, 2018 on the organization of the National Commission for the protection

data and the general data protection regime, in particular Article 41 thereof;

Having regard to the internal rules of the National Commission for Data Protection

adopted by decision no. 3AD/2020 dated January 22, 2020, in particular its article 10, point

2;

Having regard to the regulations of the National Commission for Data Protection relating to the

investigation procedure adopted by decision No. 4AD/2020 dated January 22, 2020, in particular

its article 9;

Considering the following:

I.

Facts and procedure

1.

Given the impact of the role of the Data Protection Officer (hereinafter: the “DPO”) and

the importance of its integration into the organization, and considering that the guidelines

concerning DPOs have been available since December 20161, i.e. 17 months before the entry into

application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

on the protection of individuals with regard to the processing of personal data

personal data and on the free movement of such data, and repealing Directive 95/46/EC

1 The DPO Guidelines were adopted by the Article 29 Working Party on 13

December 2016. The revised version (WP 243 rev. 01) was adopted on April 5, 2017.

Decision of the National Commission sitting in restricted formation on the outcome of

survey no.[…] conducted with Administration A

(General Data Protection Regulation) (hereinafter: the “GDPR”), the Commission

National Commission for Data Protection (hereinafter: the “National Commission” or the

“CNPD”) has decided to launch a thematic survey campaign on the function of the DPO.

Thus, 25 audit procedures were opened in 2018, concerning both the private sector and the

public sector.

2.

In particular, the National Commission decided by deliberation n°[…] of 14

September 2018 to open an investigation in the form of a data protection audit

with Administration A (hereinafter: the “controlled”) and to designate Mr. Christophe

Buschmann as chief investigator. Said deliberation specifies that the investigation relates to the

compliance of the controlled with section 4 of chapter 4 of the GDPR.

3.

4.

[…]

By letter dated September 17, 2018, the head of investigation sent a questionnaire

preliminary to the control to which the latter replied by email of October 5, 2018. Visits

on site took place on March 5 and May 2, 2019. Following these exchanges, the head of investigation established

audit report no.[…] (hereinafter: the “audit report”).

5.

It appears from the audit report that in order to verify the organization's compliance with the

section 4 of chapter 4 of the GDPR, the head of investigation has defined eleven control objectives,

to know :

1) Ensure that the body subject to the obligation to appoint a DPO has done so;

2) Ensure that the organization has published the contact details of its DPO;

3) Ensure that the organization has communicated the contact details of its DPO to the CNPD;

4) Ensure that the DPO has sufficient expertise and skills to

carry out its missions effectively;

5) Ensure that the missions and tasks of the DPO do not lead to a conflict of interest;

6) Ensure that the DPO has sufficient resources to carry out effectively

of its missions;

7) Ensure that the DPO is able to carry out his duties with a sufficient degree

autonomy within their organization;

8) Ensure that the organization has put in place measures for the DPO to be associated with

all questions relating to data protection;

9) Ensure that the DPO fulfills his mission of providing information and advice to the

controller and employees;

10) Ensure that the DPO exercises adequate control over data processing within

of his body;

11) Ensure that the DPO assists the controller in carrying out the

impact analyzes in the event of new data processing.

6.

By letter dated October 18, 2019 (hereinafter: the "statement of objections"), the head of investigation informed the control of the breaches of the obligations provided for by the RGPD that it found during his investigation. The audit report was attached to that letter.

7. In particular, the head of investigation noted in the statement of objections breaches of

~

~

~

~

~

~

~

the obligation to appoint the DPO on the basis of his professional qualities2;

the obligation to communicate the contact details of the DPO to the supervisory authority3;

the obligation to involve the DPO in all questions relating to the protection of personal data4;

the obligation to provide the necessary resources to the DPO5;

the obligation to guarantee the autonomy of the DPO6;

the information and advice mission of the DPO7;

the control mission of the DPD8.

8.

By letter dated November 22, 2019, the inspector sent the head of the investigation his decision position on the shortcomings listed in the statement of objections.

9.

On August 3, 2020, the head of investigation sent an additional letter to the controller to the statement of objections by which it informs the auditee of the corrective measures it proposes to the National Commission sitting in restricted formation (hereinafter: "the" formation restricted") to adopt. In this letter, the head of investigation proposed to the restricted formation to adopt six different corrective measures.

2 Objective 4

3 Objective 3

4 Objective 8

5 Objective 6

6 Goal 7

7 Goal 9

8 Goal #10

10.

By letter dated August 14, 2020, the person inspected sent the head of the investigation his comments on the additional letter to the statement of objections.

The case was on the agenda of the Restricted Committee meeting on January 15

11.

2021. In accordance with Article 10.2. b) the internal rules of the Commission

national, the head of investigation and the controller presented oral observations on the case and

answered the questions posed by the Restricted Committee. The controller had the floor

last.

II.

Place

A. On the breach of the obligation to designate the DPO on the basis of his qualities

professional

1. On the principles

12.

According to article 37.5 of the GDPR, “[the DPO] is appointed on the basis of his qualities

professional skills and, in particular, his specialized knowledge of the law and practices

in terms of data protection […]”.

13.

According to recital (97) of the GDPR, “[t]he level of specialist knowledge

required should be determined in particular according to the data processing operations

carried out and the protection required for the personal data processed by the

controller or processor”.

14.

In addition, the Article 29 Data Protection Working Party has adopted

on 13 December 2016 guidelines concerning DPOs which have been taken over and

re-approved by the European Data Protection Board on May 25, 20189.

These guidelines specify that the level of expertise of the DPO “must be proportionate to the

sensitivity, complexity and volume of data processed by an organization”10 and that “it

It is necessary for DPOs to have expertise in the field of legislation and

national and European data protection practices, as well as a

in-depth knowledge of the GDPR”11.

9 WP 243 v.01, version revised and adopted on April 5, 2017

10 WP 243 v.01, version revised and adopted on April 5, 2017, p. 13

11 WP 243 v.01, version revised and adopted on April 5, 2017, p. 14

The DPO Guidelines go on to state that “[k]nowledge

15.

sector of activity and organization of the data controller is useful. The DPO should

also have a good understanding of the processing operations carried out,

as well as the information systems and the needs of the data controller in terms of

data protection and security”.

2. In this case

16.

It appears from the audit report that, for the head of investigation to consider objective 4

as filled in by the controller as part of this audit campaign, the head of investigation

expects the DPO to have a minimum of three years of professional experience in

Data protection.

17.

According to the statement of objections, page 3, it was found during the investigation that “the

DPD has no initial training in legal or data protection matters, nor does it justify

of a practice in this area. The fact that the DPO has participated in 2 specific training

data protection in 2017 and attended the INAP participatory workshops in 2018, is not enough

not to establish the existence of expertise adapted to the needs of the data controller".

18.

In its position paper of November 22, 2019, the auditee asserts the will and the

ability of the DPO to learn and become familiar with new legislation, its

excellent knowledge of the operating mode of the controlled and the procedures, its meaning

keen sense of responsibility as well as his great professional conscience. […] Furthermore, the

controlled claims to have set up a close, albeit non-formal, collaboration with the

Legal Department.

19.

The Restricted Committee notes first of all that in its position paper of November 22

2019, the audit does not call into question the findings made by the head of the investigation as to

the lack of initial legal or data protection training of the DPO, and

about the DPO's lack of practice in this area.

20.

The Restricted Committee takes note of the fact that, according to the audit, the DPO has

a good understanding of the operation as well as the control procedures, […] and

that close collaboration has been established between the DPO and the legal department.

12 WP 243 v.01, version revised and adopted on April 5, 2017, p.14

Nevertheless, the Restricted Committee considers that these elements do not make it possible to establish

that the DPO has expertise adapted to the needs of the control, in particular in view of the

sensitivity, complexity and volume of data processed by the controller. Indeed, He

It appears from the statement of objections that the auditee 'manages approximately […] customers […].

Administration A also employs approximately […] staff. The body therefore treats a

substantial amount of data whose degree of sensitivity may be relatively high […]. »

21.

The Restricted Committee also takes note of the fact that in its letter of 14 August

2020, the control indicated that it was "in the process of finalizing the recruitment of a full-time DPO

and having a level of expertise adapted to the sensitivity, complexity and volume of the

data processed [by the controller]. » If such a measure should allow the controlled person to

bring into compliance, it should nevertheless be noted that this was decided during

of investigation. The Restricted Committee therefore agrees with the finding of the head of investigation according to

which, at the start of the investigation, the person audited was unable to demonstrate that he appointed

a DPO with sufficient professional qualities.

22.

The Restricted Committee further notes that if it was able to ascertain that a new DPO

has actually been appointed by the person inspected during the investigation, it does not, however, have

no documentation that would verify that he has the professional qualities

sufficient.

23.

In view of the foregoing, the Restricted Committee concludes that Article 37.5 of the GDPR has no

not respected by the controller.

B. On the failure to communicate the contact details of the DPO to the authority

control

1. On the principles

24.

Article 37.7 of the GDPR provides for the obligation for the organization to communicate the

contact details of the DPO to the supervisory authority. Indeed, it follows from Article 39.1. e) GDPR

that the DPO acts as a point of contact for the supervisory authority so it is important

that the latter has the contact details of the DPO.

25.

The DPO Guidelines explain in this respect that this requirement
aims to ensure that “supervisory authorities can easily and directly take
contact with the DPO without having to go to another department of the body”13.

26.

It should also be noted that the CNPD published on its website as of May 18
2018 a form allowing organizations to send it the contact details of their
DPD.

2. In this case

It appears from the audit report that, for the head of investigation to consider objective 3

27.

as filled in by the controller as part of this audit campaign, the head of investigation
expects the organization to have communicated the contact details of its DPO by 25 May 2018
at the CNPD.

28.

According to the statement of objections, page 3, the communication of the contact details of the
DPD to the CNPD was made on […] October 2018 through the Commissariat du
Government to the protection of data with the State, and not by the control itself
same.

29.

In its position paper of November 22, 2019, the auditee acknowledges that the

communication of the contact details of the DPO was not made according to the procedure provided for and affirms that it will ensure in the future that any possible changes concerning the DPO are communicated directly to the CNPD.

30.

The Restricted Committee notes that the GDPR has been applicable since May 25, 2018 from so that the obligation to communicate the contact details of the DPO to the supervisory authority exists since that date. Thus, the communication of the contact details of the DPO to the CNPD dated […] October 2018 was late. Furthermore, it should be noted that it is up to the organization having appointed the DPO to communicate the contact details of its DPO to the CNPD, even if the organization is, as in the present case, a State administration.

31.

In view of the foregoing, the Restricted Committee concludes that Article 37.7 of the GDPR has no not respected by the controller.

13 WP 243 v.01, version revised and adopted on April 5, 2017, p.15

C. On the breach of the obligation to involve the DPO in all matters relating to the protection of personal data

1. On the principles

According to Article 38.1 of the GDPR, the organization must ensure that the DPO is associated,

32.

in an appropriate and timely manner, to all questions relating to the protection of personal data.

33.

The DPO Guidelines state that “[i]t is essential that the DPO,

or his team, is involved from the earliest possible stage in all questions

relating to data protection. […] Information and consultation of the DPO from the start

will facilitate compliance with the GDPR and encourage a data-driven approach.

data protection by design; it should therefore be standard procedure in the

within the governance of the organization. Furthermore, it is important that the DPO be considered as

an interlocutor within the organization and that he is a member of the working groups devoted

to data processing activities within the organisation”14.

The DPO Guidelines provide examples on how

34.

to ensure this association of the DPO, such as:

-
-
-
-

invite the DPO to regularly attend management meetings

superior and intermediate;

to recommend the presence of the DPO when decisions having implications

with regard to data protection are taken;

to always give due consideration to the opinion of the DPO;

to immediately consult the DPO when a data breach or other

incident occurs.

35.

According to the DPO guidelines, the organization could, if necessary,

develop data protection guidelines or programs

indicating the cases in which the DPO must be consulted.

Decision of the National Commission sitting in restricted formation on the outcome of

survey no.[…] conducted with Administration A

8/28

2. In this case

36.

It appears from the audit report that, for the head of investigation to consider objective 8

as completed by the auditee as part of this audit campaign, he expects the

DPD participates in a formal manner and on the basis of a frequency defined by the

management, project coordination committees, new product committees,

security committees or any other committee deemed useful in the context of data protection.

37.

According to the Statement of Objections, pages 3 and 4, the DPO is informed of new

projects informally and provides an informal update on data protection issues

with [the Management] of the control every 15 days. The Statement of Objections further indicates

that "[t]he fact that the integration of a GDPR module into the project methodology is in progress

is not sufficient to establish the existence of an organized association of the DPO in matters relating

to data protection, nor is it likely to establish the position of the DPO as

as interlocutor within the organization. »

38.

In its position paper of November 22, 2019, the auditee argues that it is before

all of a lack of formalization on his part and that the DPO is associated with issues relating

to the protection of personal data insofar as it is consulted by the heads of

projects and management “as soon as they identify processing activities that risk

include personal data”. According to the control, the DPD is also

invited “to all meetings in which questions relating to the protection of

personal data are on the agenda, including the management committee”. By

elsewhere, the control indicates that the DPO answers any questions from employees

control over this.

39.

The Restricted Committee recognizes that the GDPR does not specify what measures

which should be taken by the data controller to ensure the association of the DPO

to all questions relating to data protection. Guidelines for

however, the DPOs formulate recommendations and good practices, in order to guide the

controllers in complying with their governance in

in particular providing examples on how to ensure this association.

40.

The Restricted Committee also notes that it is rightly specified on page 2 of the

statement of objections (under “preliminary remarks”) that “[t]he requirements of the GDPR

are not always strictly defined. In such a situation, it is up to the authorities to

control to verify the proportionality of the measures put in place by the persons in charge of

processing with regard to the sensitivity of the data processed and the risks incurred by the

persons concerned. »

41.

However, the Restricted Committee notes that it is also specified in the communication of the

grievances that the controlled “manages about […] customers […]. [The controlled] also employs about

[…] collaborators. " The head of investigation concludes that "The organization therefore treats a number

substantial amount of data, the sensitivity of which may be relatively high, such as […]. »

The Restricted Committee shares this assessment. The Restricted Committee therefore considers that the formalized and systematic participation of the DPO in relevant meetings, as is expected by the head of the investigation, constitutes a proportionate measure in order to ensure involving the DPO in all questions relating to the data protection of personal.

42.

The Restricted Committee takes note of the fact that in its position paper of 22 November 2019, the control indicates that it was decided “to further formalize the participation [of the] DPD to activities. [The DPO] is thus now automatically a member of the steering committee of all projects [of the auditee] (projects already in progress and new projects)” and also takes note of the fact that in his letter of August 14, 2020, the controller further specifies that in the event of the absence of the DPD in a meeting "the minutes are sent to him and, if necessary, an interview between the project manager and the DPO is organised. » If these measures should facilitate the association of the DPD to all questions relating to data protection, it should nevertheless be note that these were decided during the investigation. The restricted formation rallies consequently to the finding of the head of the investigation that, at the start of the investigation, the controller was unable to demonstrate that the DPO was associated with appropriate manner, to all questions relating to the protection of personal data.

43.

The Restricted Committee also notes that it does not have the documentation which would make it possible to demonstrate that the measures described by the controller would have been implemented work.

In view of the foregoing, the Restricted Committee concludes that Article 38.1 of the GDPR has no

44.

not been respected.

D. On the failure to provide the necessary resources to the DPO

1. On the principles

45.

Article 38.2 of the GDPR requires the organization to help its DPO “to carry out the tasks referred to in Article 39 by providing the resources necessary to carry out these tasks, as well as that access to personal data and processing operations, and to maintain their specialist knowledge. »

46.

It follows from the DPO Guidelines that the following aspects should in particular be taken into consideration15:

~ “sufficient time for DPOs to perform their tasks. This aspect is particularly important when an internal DPO is appointed on a part-time or when the external DPO is in charge of data protection in addition to other tasks. Otherwise, conflicting priorities could lead to the tasks of the DPD are neglected. It is essential that the DPO can devote enough time on his assignments. It is good practice to set a percentage of time devoted to the function of DPO when this function is not occupied full time. It is also good practice to determine the time required to complete the the appropriate function and level of priority for the DPO's tasks, and that the DPO (or organization) draw up a work plan;

~

necessary access to other services, such as human resources, the service

legal, IT, security, etc., so that DPOs can

receive essential support, input and information from these other

services ".

47.

The DPO Guidelines state that “[b]eally,

the more complex or sensitive the processing operations, the more resources allocated

to the DPO will have to be significant. The data protection function must be effective and

equipped with adequate resources with regard to the data processing carried out. »

15 WP 243 v.01, version revised and adopted on April 5, 2017, p. 17

---

2. In this case

48.

It appears from the audit report that, given the size of the organizations selected in the

framework of this audit campaign, so that the head of investigation considers objective 6 as

filled in by the person being controlled, the head of investigation expects the person being controlled to have at least one FTE

(full-time equivalent) for the data protection team. Leader

of investigation also expects the DPO to have the possibility of relying on other

services, such as legal, IT, security, etc.

49.

According to the Statement of Objections, page 4, “[i]t appears from the investigation that the DPO is

affected at 25% (approximately 10 hours per week). The DPO carries out its tasks alone. The fact that the

DPD benefits from the informal support of the legal department and the IT department and

that an external service provider has intervened for 60 man-days over a period of 12 months (i.e. approximately 5 days per month), would not be sufficient to provide sufficient time for the DPO accomplishes his tasks. The statement of objections goes on to state that 'the controller has not been able to demonstrate the fulfillment of the control or information and advice missions of the DPO (see development in point 3). This finding is likely to highlight a mismatch between the resources and means made available to the DPO and the needs of the controller. »

50.

In its position paper of November 22, 2019, the auditee takes note of the observation made by the head of investigation that the DPO does not have the necessary resources to accomplish its missions. The controlled maintains however that "even if it is informal, the collaboration with the Legal Department is real and allows our DPO to benefit from additional resources. According to the control, these resources are estimated at approximately 5 hours per week.

51.

The Restricted Committee notes that it appears from the investigation file that the DPO was also head of the department […] and devoted about 10 hours a week to his tasks of DPD. Even taking into consideration the support provided by the legal department and the IT as well as the temporary intervention of an external service provider, restricted training considers that the DPO did not have sufficient time to perform his tasks, this particularly with regard to the sensitivity, complexity and volume of the data processed by Control.

52.

In his letter of August 14, 2020, the controller indicates that a full-time DPO is in recruitment course, that he “will have internal support (from the legal department, the

IT and the current DPO)" and that a budget envelope is envisaged for a
external medium.

53.

Whether the Restricted Committee has been able to verify that a new DPO has actually been appointed by the inspection during the investigation, it nevertheless does not have the documentation that would make it possible to verify that it has sufficient resources, and in particular that the DPO works full time.

54.

In view of the foregoing, the Restricted Committee concludes that Article 38.2 of the GDPR has no not respected by the controller.

E. On the breach of the obligation to guarantee the autonomy of the DPO

1. On the principles

55.

Under Article 38.3 of the GDPR, the organization must ensure that the DPO "not receive any instructions with regard to the exercise of the missions". Furthermore, the DPO "reports directly to the highest level of management" of the organization.

56.

Recital (97) of the GDPR further states that DPOs "should be able to exercise their functions and missions in full independence".

57.

According to the DPO Guidelines16, Article 38.3 of the GDPR "provides certain basic safeguards intended to ensure that DPOs are able to exercise their missions with a sufficient degree of autonomy within their organization. […] That

means that, in the exercise of their tasks under Article 39, DPOs must not

receive instructions on how to handle a case, for example, what outcome should be

obtained, how to investigate a complaint or whether to consult the supervisory authority.

Furthermore, they cannot be required to adopt a certain point of view on a matter related to the

data protection legislation, for example, a particular interpretation

law. […] If the controller or processor makes decisions that are

incompatible with the GDPR and the opinion of the DPO, the latter should have the possibility to indicate

clearly his opinion diverges at the highest level of management and to decision makers. In this

In this respect, Article 38(3) provides that the DPO "reports directly to the level most

higher than the management of the controller or the processor". Such a surrender

direct account ensures that senior management (e.g. board of directors) has

16 WP 243 v.01, version revised and adopted on April 5, 2017, p. 17 and 18

---

knowledge of the opinions and recommendations of the DPO which are part of the

mission of the latter consisting in informing and advising the data controller or the

subcontracting. The preparation of an annual report on the activities of the DPO intended for the

management is another example of direct accountability. »

2. In this case

58.

It appears from the audit report that, for the head of investigation to consider objective 7

as filled in by the controller as part of this audit campaign, the head of investigation

expects the DPO to be "reported to the highest level of management to ensure the

maximum autonomy.

59.

According to the Statement of Objections, p. 4, “[i]t appears from the investigation that the DPO was initially attached to the deputy director, an attachment which was not formalized. Otherwise, Administration A has not been able to demonstrate the existence of a direct relationship at the level highest in management. In particular, there is no tool, such as an activity report, which could have enabled the DPO to send formal advice to the controller. In investigation, the Administration presented CNPD officials with an organizational chart showing the direct attachment of the DPO to [the Management]. This change allows to document the organization's desire to comply, but this change does not is not enough on its own to remove the breach, however noted at the start of the investigation. In Indeed, the data controller has not been able to demonstrate that the DPO could act without receiving instructions with regard to the exercise of its missions. »

60.

In its position paper of November 22, 2019, the controller argues that the DPD is from now on formally attached directly to the [Direction] of the controlled in organization chart and asserts in particular that the DPO "does not receive instructions concerns the exercise of its tasks referred to in Article 39, and it obtains the support of the responsible for the processing in order to be able to exercise them independently”.

61.

As to the possibility for the DPO to address formal advice which would contribute to demonstrate, in the words of the head of the investigation, "the existence of a direct report at the highest level highest level of management", the Restricted Committee notes that it appears from the investigation file

that the DPO participates in informal meetings with management17 and that the DPO takes stock

informal on data protection issues with [Management] every 15 days18.

17 Visit report of 5 March 2019, point 8

18 Statement of Objections, p. 3

The Restricted Committee notes that, given the informal nature of these DPO contacts

with management, these elements do not tend to demonstrate the existence of a direct relationship with the

highest level of management.

62.

Moreover, with regard to the hierarchical attachment, if it does not result from the

provisions of the GDPR that the DPO must necessarily be attached to the highest level

of the management in order to guarantee its autonomy, the restricted committee nevertheless reminds

that it has noted in point 40 of this decision that it is rightly stated on page 2 of

the statement of objections (under "preliminary remarks") that "[t]he requirements of the

GDPR are not always strictly defined. In such a situation, it is up to the

supervisory authorities to verify the proportionality of the measures put in place by the

data controllers with regard to the sensitivity of the data processed and the risks

incurred by the persons concerned. »

63.

However, as mentioned in point 41 of this decision, the training

management shares the assessment of the head of investigation, mentioned on page 2 of the

statement of objections, according to which the audited "handles […] a substantial number of

data whose degree of sensitivity may be relatively high […]". Restricted training

therefore considers that, in the absence of other measures which would make it possible to demonstrate that the DPD is able to circumvent the intermediate hierarchical levels as soon as it deems it necessary, the hierarchical reporting of the DPO to the highest level of management, according to expectation of the head of investigation, constitutes a proportionate measure in order to guarantee his autonomy. In this regard, the Restricted Committee notes that the attachment of the DPO to the top level of management was not decided by the control until after the start of the investigation.

64.

In view of the foregoing, the Restricted Committee agrees with the finding of the head of investigation that, at the start of the investigation, the data controller was unable to demonstrate that the DPO could act without receiving instructions with regard to the exercise of its missions.

65.

In view of the foregoing, the Restricted Committee concludes that Article 38.3 of the GDPR has no not been respected by the controller.

F. On the breach relating to the mission of information and advice of the DPO

1. On the principles

66.

Under Section 39.1. a) of the GDPR, one of the tasks of the DPO is to “inform and advise the controller or processor as well as the employees who carry out processing on their obligations under this Regulation and other provisions of Union law or the law of the Member States relating to the protection of data ".

2. In this case

67.

It appears from the audit report that, for the head of investigation to consider objective 9

as filled in by the controller as part of this audit campaign, the head of investigation

expects “the organization to have formal reporting of activities from the DPO to the

Management Committee on the basis of a defined frequency. Regarding employee information,

it is expected that the organization has set up an adequate staff training system

on data protection”.

68.

On these two points, according to the Statement of Objections, page 5, “[i]t is apparent from

the investigation that there is no tool such as an activity report which could have enabled the DPO

send formal advice to the data controller. Furthermore, the staff of

Administration A receives awareness sessions on IT security,

but no awareness of data protection in general. The manager of

processing has not been able to demonstrate that the DPO carries out its information tasks

and advice, both with regard to the data controller himself and with regard to employees

who carry out the processing operations. »

69.

In its position paper of November 22, 2019, the controller argues that the DPD has

advised the management of the organization on the obligations incumbent upon it in terms of protection

data, “even if this advice was not formally documented”. Control

further indicates that “[a] GDPR compliance project was launched in 2017 and

different steps were listed on a graph which served as a basis for the DPD and the Management

to set priorities. On the other hand, the progress of the project has not actually been the subject of

of documentation. […] Finally, the auditee maintains that the DPD advised its agents to

any question relating to data protection, “even if specific training on

this subject have not yet taken place" and indicates that "[t]he heads of departments and the collaborators

were encouraged to contact the DPO individually for any information and advice
about data protection. »

70.

The Restricted Committee notes that Article 39.1 of the GDPR lists the missions that the
DPD must at least be entrusted with the task of informing and advising the organization as well as
employees, without however specifying whether specific measures should be implemented.
place to ensure that the DPO can fulfill his mission of information and advice. The
guidelines for DPOs, which provide recommendations and good
practices to guide data controllers in compliance with the
their governance, also only briefly address the mission of advising and
information from the DPO. Thus, they specify that the keeping of the register of processing activities
referred to in Article 30 of the GDPR may be entrusted to the DPO and that “[t]his register must be considered
as one of the tools allowing the DPO to carry out its tasks of monitoring compliance with the
GDPR as well as information and advice to the controller or sub-
dealing.19”

71.

With regard to the mission of information and advice with regard to the person in charge of the
processing, it appears from the investigation file that the DPO was involved in establishing the
record of processing activities20, that it participates in informal meetings with the
management21, that access to management is easy for the DPO22 and that the DPO makes an informal point
on data protection issues with [Management] every 15 days23.

72.

Nevertheless, the Restricted Committee recalls that it has already noted in point 40 of the

this decision that page 2 of the statement of objections (under

“preliminary remarks”) that “[t]he GDPR requirements are not always strictly

defined. In such a situation, it is up to the supervisory authorities to verify the

proportionality of the measures put in place by the data controllers with regard to

the sensitivity of the data processed and the risks incurred by the persons concerned. »

73.

However, as mentioned in point 41 of this decision, the training

management shares the assessment of the head of investigation, mentioned on page 2 of the

statement of objections, according to which the audited "handles […] a substantial number of

data whose degree of sensitivity may be relatively high […]”. Restricted training

19 WP 243 v.01, version revised and adopted on April 5, 2017, p. 22

20 Visit report of March 5, 2019, p. 2

21 Visit report of 5 March 2019, point 8

22 Visit report of 5 March 2019, point 8

23 Statement of Objections, p. 3

therefore considers that formal reporting of the activities of the DPO to the management, on the

based on a defined frequency, is a proportionate measure to demonstrate that the

DPD carries out its missions of information and advice with regard to the data controller.

74.

The Restricted Committee takes note of the fact that the controller indicated in his letter

of 14 August 2020 that it was decided to set up formal reporting of the activities of the DPO
(on a quarterly basis which may be reviewed and adapted if necessary). Training
limited, which does not have the documentation that would demonstrate the implementation
implementation of this measure, notes that it was decided during the investigation and agrees by
consequent to the finding of the head of investigation that, at the start of the investigation, the person in charge
processing has not been able to demonstrate that the DPO carries out its tasks
information and advice with regard to the data controller.

75.

As for the mission of information and advice with regard to employees, the training
Restricted notes that it appears from the investigation file24 that:

~ approximately […] control officers have been trained in IT security;

~ the code of conduct and the training relating to […] contain elements relating to the
Protection of personal data ;

~ personnel assigned […] to control have been trained to prevent unauthorized disclosure
authorized information; and

~ a training plan integrating aspects relating to data protection and
destination of all control agents is planned for the end of 2019/beginning of 2020.

76.

In its position paper of November 22, 2019, the auditee indicates that "Des
specific training courses on the protection of personal data are being

organized and will take place in 2020."

77.

The Restricted Committee also notes that the controller indicated in his letter of the August 14, 2020 that "[t]he internal training of employees on the GDPR and the data protection (…) began during the first quarter of 2020" and that these training courses "are compulsory for all employees and will be organized regular way". The Restricted Committee nevertheless notes that it does not have the documentation that would demonstrate the implementation of this measure.

24 Visit report of 5 March 2019, point 9

78.

In view of the elements mentioned above in point 75 of this Decision which emerge from the investigation file as well as from the indications provided by the person inspected in his decision of position of November 22, 2019 and in its letter of August 14, 2020, the Restricted Committee notes that, at the time of the opening of the investigation, the staff of the control was not specifically aware of data protection.

79.

The Restricted Committee therefore agrees with the finding of the head of investigation according to which, at the start of the investigation, the data controller was unable to demonstrate that the DPO carries out its missions of information and advice with regard to employees who carry out the processing operations.

80.

The Restricted Committee also points out that it does not have the documentation

which would make it possible to demonstrate that the measures decided by the control, mentioned in points 74 and 77 of this decision have been implemented.

81.

In view of the foregoing, the Restricted Committee concludes that Article 39.1. a) GDPR was not respected by the controller.

G. On the breach relating to the control mission of the DPO

1. On the principles

82.

According to Article 39.1. b) of the GDPR, the DPO has, among other things, the mission of “monitoring the compliance with this Regulation, other provisions of Union law or national law members with regard to data protection and the internal rules of the data controller processing or of the processor with regard to the protection of personal data, including including with regard to the distribution of responsibilities, awareness and training personnel involved in processing operations, and related audits”. the recital (97) clarifies that the DPO should help the body to verify compliance, at the level internal, GDPR.

83.

It follows from the DPO Guidelines25 that the DPO can, within the framework of these control tasks, in particular:

~ collect information to identify processing activities;

~ analyze and verify the compliance of processing activities;

25 WP 243 v.01, version revised and adopted on April 5, 2017, p. 20

inform and advise the controller or processor and formulate
recommendations to him.

2. In this case

84.

It appears from the audit report that, for it to be able to consider objective 10 as fulfilled
audited as part of this audit campaign, the head of investigation expects that
“the organization has a formalized data protection control plan
(even if not yet executed)”.

85.

According to the Statement of Objections, p. 5, “[i]t appears from the investigation that the organization
does not monitor compliance with GDPR rules and does not have a control plan. " Leader
investigation refers in particular to the answer provided by the auditee to question 5 c) of the
preliminary questionnaire26. The controller indicates that “[c]urrently monitoring the
compliance with the rules does not apply, an audit plan will be drawn up in 2019.”

86.

In its position paper of November 22, 2019, the auditee argues that the DPD was
at the time of the investigation writing […] a [document] […] which “corresponds to a plan of
control, since it analyzes the obligations that the GDPR imposes on the data controller
and explains the steps taken to comply and the actions that remain to be
put in place ". The auditee indicates that "these actions have not been formally addressed
to the controller, e.g. by means of an action plan, but the most important points

urgent matters were raised during the exchanges between the [Management] and the DPO". The control indicates also that "[t]he DPO checks at the end of the year whether the compliance actions reported to the different services have been put in place" and that "the results of these checks will be documented in an audit report. »

87.

The Restricted Committee notes that Article 39.1 of the GDPR lists the missions that the DPO must at least be entrusted with the task of monitoring compliance with the GDPR, without however, require the organization to put in place specific measures to ensure that the DPD can fulfill its control mission. DPO guidelines indicate in particular that the keeping of the register of processing activities referred to in Article 30 of the GDPR can be entrusted to the DPO and that "[t]his register should be considered as one of the

26 How does the DPO monitor compliance? Please describe

tools allowing the DPO to carry out its missions of monitoring compliance with the GDPR as well as information and advice from the controller or processor.27"

88.

The Restricted Committee has already noted in point 71 of this decision that it is clear from the investigation file that the DPO was involved in the establishment of the register of the activities of treatment28. The Restricted Committee nevertheless notes that this element taken in isolation is not sufficient not have to demonstrate that the DPO carries out its task of monitoring compliance with the GDPR in a adequate.

89.

The Restricted Committee recalls that it has noted in point 40 of this decision

that it is rightly stated on page 2 of the statement of objections (under “remarks

preliminary”) that “[t]he requirements of the GDPR are not always strictly defined.

In such a situation, it is up to the supervisory authorities to verify the proportionality of the

measures put in place by the data controllers with regard to the sensitivity of the

data processed and the risks incurred by the persons concerned. »

90.

However, as mentioned in point 41 of this decision, the training

management shares the assessment of the head of investigation, mentioned on page 2 of the

statement of objections, according to which the audited "handles […] a substantial number of

data whose degree of sensitivity may be relatively high […]”.

91.

The Restricted Committee therefore considers that the inspection mission carried out

by the DPO to the controller should be formalized, for example by a control plan in

data protection, in order to be able to demonstrate that the DPO carries out his mission

adequate monitoring of GDPR compliance.

92.

However, it appears from the investigation file and the elements communicated by the person inspected in

its position paper of 22 November 2019 that the control mission carried out by the DPD

was not formalized at the time of the opening of the investigation.

93.

The Restricted Committee takes note of the fact that in its letter of 14 August 2020, the

controlled states that "[t]he measure to order the deployment of the DPD's control mission

through a control plan and control reports is retained. A control plan

annual must be provided by the [DPO] at the end of each year for the following year, together

with the inspection reports of the past year. Nevertheless, this decision having been taken

27 WP 243 v.01, version revised and adopted on April 5, 2017, p. 22

28 Visit report of March 5, 2019, p. 2

Decision of the National Commission sitting in restricted formation on the outcome of

survey no.[…] conducted with Administration A

21/28

during the investigation, the Restricted Committee agrees with the finding of the head of investigation that

the controlled party has not been able to demonstrate that the DPO carries out its control tasks

GDPR compliance.

94.

The Restricted Committee also notes that it does not have the documentation

which would make it possible to demonstrate that this measure was put in place by the controller.

95.

In view of the foregoing, the Restricted Committee concludes that Article 39.1. b) GDPR

was not respected by the controller.

III.

On corrective measures

A. Principles

96. In accordance with article 12 of the law of 1 August 2018 organizing the

National Commission for Data Protection and the General Data Protection Regime

data protection, the National Commission has the powers provided for in Article

58.2 GDPR:

(a) notify a controller or processor of the fact that the operations of

envisaged processing are likely to violate the provisions of this

settlement;

(b) call a controller or processor to order when the

processing operations have resulted in a breach of the provisions of this

settlement;

(c) order the controller or processor to comply with requests

submitted by the data subject with a view to exercising their rights under this

this Regulation;

d) order the controller or the processor to put the operations of

processing in accordance with the provisions of this Regulation, where applicable,

specifically and within a specified time;

(e) order the controller to communicate to the data subject a

personal data breach;

---

f)

impose a temporary or permanent limitation, including a ban, on the

treatment;

g) order the rectification or erasure of personal data or the

limitation of processing pursuant to Articles 16, 17 and 18 and the notification of these

measures to the recipients to whom the personal data have been

disclosed pursuant to Article 17(2) and Article 19;

(h) withdraw a certification or order the certification body to withdraw a

certification issued pursuant to Articles 42 and 43, or order the body to

certification not to issue certification if the requirements applicable to the

certification are not or no longer satisfied;

i)

impose an administrative fine pursuant to Article 83, in addition to or in

instead of the measures referred to in this paragraph, depending on the characteristics

specific to each case;

j) order the suspension of data flows addressed to a recipient located in a

third country or an international organisation. »

97.

These measures also include the power to "impose an administrative fine in

application of Article 83 (…)". However, article 48, paragraph 1, of the law of 1 August 2018 on

organization of the National Commission for Data Protection and the general regime

on data protection specifies that "[t]he CNPD may impose fines

administrative procedures as provided for in Article 83 of the [GDPR], except against the State or

communes" (emphasis added).

98.

The Restricted Committee would like to point out that the facts taken into account in the context of the

this Decision are those found at the start of the investigation. Nevertheless, the procedures

performed by the controller to comply with the GDPR during the procedure

of investigation or to remedy the shortcomings noted by the head of investigation in the

statement of objections are taken into account by the Restricted Committee within the framework of the

any corrective measures to be taken.

B. In the instant case

1. As to taking corrective action

99.

In its supplementary letter to the statement of objections of 3 August 2020, the

head of investigation proposes to the restricted committee to take corrective measures following:

"a) Order the implementation of measures allowing the DPO (or a "Data Protection" dedicated) to acquire sufficient expertise adapted to the needs of the data protection controller in accordance with the provisions of Article 37, paragraph (5) of the GDPR and the guidelines relating to the DPO of the "article 29" working party on data protection which specifies that the level of expertise of the DPO must be proportionate to the sensitivity, complexity and the volume of data processed by the organization. Although several ways could be considered to achieve this result, one of the possibilities would be to provide formal internal or external support to the DPO in legal matters and in information system security.

b) Order the implementation of measures ensuring that for any modification later by the DPO, the declaration to the data protection authority either made in time by the data controller himself, in accordance with Article 37 paragraph (7) of the GDPR.

c) Order the implementation of measures ensuring formal and effective association of the DPO on all questions relating to data protection, in accordance the requirements of Article 38 paragraph 1 of the GDPR. Although several ways could be considered to achieve this result, one of the possibilities would be analyze, together with the DPO, all relevant committees/working groups with regard to data protection and to formalize the terms of its intervention (previous meeting agenda information, invitation, frequency, status of permanent member, etc.).

d) Order the provision of the necessary resources to the DPO in accordance with the requirements of Article 38 paragraph 2 of the GDPR. Although several ways

could be considered to achieve this result, one of the possibilities would be
to relieve the DPO of all or part of his other missions/functions or to provide him with
formal support, internally or externally, regarding the exercise of its missions of
DPD.

e) Order the deployment of the DPO control mission, in accordance with Article
39 paragraph 1 b) GDPR. Although several ways can be envisaged
to achieve this result, the DPO should document his controls over the application
internal data protection rules and procedures (second
line of defense). This documentation could take the form of a control plan
suid of control or audit reports.

f) Order the implementation of measures allowing the DPO to inform and advise
formally the data controller and the employees (who carry out the
processing) on their data protection obligations, in accordance with
to Article 39 (1) (a) GDPR. Although several ways can be
envisaged to achieve this result, one of the possibilities would be to put in place
formal reporting of the DPO's activities to Management on the basis of a frequency
defined. On the other hand, with regard to information to employees, one possibility would be to
put in place an adequate staff training system in terms of
Data protection. »

100. As for the corrective measures proposed by the head of investigation and by reference to the
point 98 of this decision, the Restricted Committee takes into account the procedures
carried out by the controlled in order to comply with the provisions of articles 37.5, 37.7,

38.1, 38.2, 39.1.a and 39.1.b of the GDPR, in particular the measures described in his letter of August 14, 2020. More specifically, it notes the following facts:

- With regard to the violation of Article 37.5 of the GDPR, the audited indicated to be "in the process of finalizing the recruitment of a full-time DPO with a level of expertise adapted to the sensitivity, complexity and volume of the data processed [for Control]. » If the restricted committee has been able to verify that a new DPO has been appointed the controlled, it does not however have the documentation which would make it possible to check that he has sufficient professional qualifications. The Restricted Committee considers as soon as it is necessary to pronounce the corrective measure proposed by the head of investigation under a).

- With regard to the violation of Article 37.7 of the GDPR, the Restricted Committee was able check that the contact details of the new DPO designated by the control have been communicated in accordance with Article 37.7 of the GDPR. The Restricted Committee considers when there is no need to pronounce the corrective measure proposed by the chief investigation under b).
- With regard to the violation of Article 38.1, measures have been decided by the monitored to ensure involvement of the DPO in all matters relating to the protection Datas. Indeed, the audit decided to "further formalize the participation [from] DPO to activities. [The DPO] is therefore now an ex officio member of the steering committee of all the projects [of the auditee] (projects already in progress and new projects)" and specified that in the event of the DPO's absence from a meeting "the minutes are sent to him and the case if necessary, an interview between the project manager and the DPO is organised. Nevertheless, the

restricted training does not have the documentation to demonstrate the taking
such compliance measures by the auditee. The Restricted Committee considers
as soon as it is necessary to pronounce the corrective measure proposed by the head of investigation
under c).
- Regarding the violation of Article 38.2, the audited indicated that a DPO “to
full time is being recruited”, that he “will have internal support (from the service
legal department, the IT department and the current DPO)” and that a budget envelope
was being considered for external support. If the Restricted Committee was able to verify that a
new DPO has been appointed by the audit during the investigation, it does not, however, have
no documentation that would verify that he has sufficient resources,
and in particular that the DPO performs his duties on a full-time basis. Restricted training
therefore considers that it is appropriate to pronounce the corrective measure proposed by the Chief
investigation under d).
- With regard to the violation of Article 39.1.a of the GDPR, with regard to the
mission of information and advice with regard to the controller, the controller has
indicated that it was decided to put in place formal reporting of the activities of the DPO (on
a quarterly basis that can be reviewed and adapted if necessary). For which
is of the mission of information and advice with regard to the employees, the control indicated
that “[t]he internal training of employees on the GDPR and the protection
data (…) started during the first quarter of the year 2020” and that these
training “are compulsory for all employees and will be organized in a way

regular”. However, the restricted formation does not have the documentation

making it possible to demonstrate the implementation of these compliance measures by the control. The Restricted Committee therefore considers that it is necessary to pronounce the measure correction proposed by the head of investigation under f).

- With regard to the violation of Article 39.1.b of the GDPR, the audited indicated that "[t]he measure to order the deployment of the DPD monitoring mission through a control plan and control reports is retained. An annual control plan should be provided by the [DPD] at the end of each year for the following year, together with the last year's inspection reports. ". Nevertheless, the restricted formation does not have no documentation demonstrating the implementation of this security measure compliance by the controller. The Restricted Committee therefore considers that there is to pronounce the corrective measure proposed by the head of investigation under e).

In view of the foregoing developments, the National Commission sitting in restricted formation and deliberating unanimously decides:

- to retain the breaches of Articles 37.5, 37.7, 38.1, 38.2, 38.3, 39.1 a) and 39.1 b) of the GDPR;

- to pronounce against Administration A, an injunction to comply with Article 37.5 of the GDPR, within four months of notification of the decision of the restricted training, the proof of compliance must be sent to the restricted training at the latest within this period, in particular: ensure that the DPO has sufficient professional qualities to exercise his or her assignments;

- to pronounce against Administration A, an injunction to comply with Article 38.1 of the GDPR, within four months of notification of the decision of the restricted training, the proof of compliance must be sent to the restricted training at the latest within this period, in particular: ensure the formalized and documented association of the DPO with all matters relating to

data protection;

- to pronounce against Administration A, an injunction to comply
with Article 38.2 of the GDPR, within four months of notification of the decision
of the restricted training, the proof of compliance must be sent to the
restricted training at the latest within this period, in particular:
ensure that the DPO has the necessary resources to carry out his duties;
- to pronounce against Administration A, an injunction to comply
with Article 39.1.a of the GDPR, within four months of notification of the
decision of the Restricted Committee, the supporting documents for compliance must be
addressed to the restricted training at the latest within this period, in particular:
ensure that the DPO exercises, in a formal and documented manner, his mission of information and
advice with regard to the data controller as well as with regard to employees;
- to pronounce against Administration A, an injunction to comply
with Article 39.1.b of the GDPR, within four months of notification of the
decision of the Restricted Committee, the supporting documents for compliance must be
addressed to the restricted training at the latest within this period, in particular:
ensure the formal and documented deployment of the DPO's control mission.

Thus decided in Belvaux on June 29, 2021.

The National Commission for Data Protection sitting in restricted formation

Tine A. Larsen Thierry Lallemang

President

Commissioner

Marc Lemmer

Commissioner

Indication of remedies

This administrative decision may be subject to an appeal for review within three months following its notification. This appeal is to be brought before the administrative court and must must be introduced through a lawyer at the Court of one of the Bar Associations.
