Decision of the National Commission sitting in restricted formation on

the outcome of survey no.[…] conducted with “Foundation A”

Deliberation no. 29FR/2021 of August 4, 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:

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

survey no.[…] conducted with “Foundation A”

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
(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 “Foundation A” established and having its registered office at […], L-[…] and registered in the register
du commerce et des société luxembourgeois under the number[…] (hereinafter: the “controlled”) and of
appoint Mr. Christophe Buschmann as head of investigation. This deliberation specifies that
the investigation concerns the compliance of the control with section 4 of chapter 4 of the GDPR.

3.

4.

According to article 2 of its statutes, the purpose of the control is [to offer social services].
By letter dated September 17, 2018, the head of investigation sent a questionnaire
preliminary to the control to which the latter replied by letter of October 5, 2018. A visit
on site took place on February 13, 2019. Following these exchanges, the head of investigation established the
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;

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.

---

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 provide the necessary resources to the DPO3;

the obligation to guarantee the autonomy of the DPO4;

the obligation to ensure that the other missions and tasks of the DPO do not lead to conflict of interest5;

the control mission of the DPO6;

the information and advice mission of the DPO7.

2 Objective 4

3 Objective 6

4 Objective 7

5 Goal 5

6 Goal #10

7 Goal 9

8.

By letter dated November 14, 2019, the inspector sent the head of the investigation his decision position on the failings noted 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 he informs the auditee of the corrective measures and the administrative fine that it proposes to the National Commission sitting in formation (hereinafter: “the “restricted formation”) to adopt. In this letter, the head of investigation proposed to the Restricted Committee to adopt five different corrective measures, as well as to impose on the person controlled an administrative fine of 17,700 euros.

10.

By letter dated August 19, 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 the investigation and the controller presented their oral observations in support of their written observations and answered the questions posed by the Restricted Committee. the controlled had the last word.

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, 20188.

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”9 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”10.

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

DPD has at least three years of professional experience in data protection

data.

17.

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

DPD "has less than 3 years of professional experience in data protection

data" and that he "does not himself have any legal expertise. ". The head of investigation

also specifies that the DPO has access to a law firm if necessary, but that “this

access is subject to the approval of the hierarchy of the DPO”. The chief investigator concludes

that “there is therefore a risk that the DPO will not be able to access the legal expertise

he needs it though. »

18.

In its position paper of November 14, 2019, the auditee indicates that it has taken "the

decision to hire a new DPO with extended powers (competences

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

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

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

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

---

legal; technical skills) as well as proven experience and a course

professional more in line with the role of DPO". The control specifies that the new DPD,

whose CV was communicated as an appendix to its position paper of November 14, 2019, was

hired and appointed on November 13, 2019.

19.

The Restricted Committee notes first of all that in its position paper of November 14

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

the professional data protection experience of the DPO who was in charge of

function at the time of the opening of the investigation. She also notes that he is not either

disputed by the controller that the DPO could encounter difficulties in accessing the expertise

legal support he needed, access to external legal support being conditional on

the approval of the hierarchy of the DPO.

20.

The Restricted Committee then notes 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 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. »

21.

However, the Restricted Committee notes that it is also specified on page 2 of the

statement of objections, that the controlled "[...]", that the activity of [...] and that the controlled

“employs approximately […] employees”. The head of the investigation concludes that the controller is dealing with a

substantial amount of data whose degree of sensitivity may be relatively high, such as

than medical data. The Restricted Committee shares this assessment and considers

since the level of expertise of the DPO who was in office at the time of the opening of

the survey was not sufficient given the sensitivity of the data processed.

22.

The Restricted Committee takes note of the fact that a new DPO, with a

sufficient expertise in data protection, and whose CV has been communicated

by the controlled with its position paper of November 14, 2019, has been designated

of investigation. If such a measure should allow the auditee to come into compliance, it

should nevertheless be noted that this was decided during the investigation. Training

restricted therefore agrees with the observation of the head of the investigation that, at the beginning of

investigation, the auditee was unable to demonstrate that he appointed a DPO with the

sufficient professional qualifications.

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 provide the necessary resources to the DPO

1. On the principles

24.

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. »

25.

It follows from the DPO Guidelines that the following aspects should in particular to be taken into consideration12:

~ “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 ".

26.

The DPO Guidelines state that “[b]eally,

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

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

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

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

2. In this case

27.

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

completed by the person being controlled, he expects the person being controlled to have at least one ETP (equivalent time

full) for the data protection team. The chief investigator expects

also that the DPO has the possibility of relying on other services, such as the

legal department, IT, security, etc.

28.

According to the audit report, the DPO performs his function "up to 0.5 FTE". He is

further specified that the DPO has “the support of an external service provider, specialized in

matters of data protection”.

29.

In the statement of objections, page 3, the head of investigation specifies that "Account

given the existence of complex or sensitive processing operations (see remarks

preliminary), a high level of resources is expected. ". However, the head of the investigation notes

that "the DPO is assigned 50%", that he "exercises his missions alone" and that the fact that it “benefits from the support of an external service provider, specialized in the protection of data, may not be sufficient to provide sufficient time for the DPO to fulfill its assignments. »

30.

In its position paper of November 14, 2019, the controller indicates that the DPD newly appointed "is assigned full-time to the various missions for which he is responsible as DPO”. The controller also indicates that the DPO “however also assists the […] in its control and audit missions. Finally, the controller specifies that the DPO has the possibility of use “external legal expertise” as well as “specialized external service providers on data protection”.

31.

Nevertheless, in its response of August 19, 2020 to the additional letter, the controller provides details on the time devoted by the DPO to the performance of his duties and indicates in particular that he “carries out his mission as DPO over a period of 80% of his time. The remaining 20% consists of assisting the […] in contract management with the external stakeholders. »

32.

It should first be noted that the Restricted Committee shares the assessment of the Chief of inquiry formulated on page 3 of the statement of objections according to which “In view of of the existence of operations of

complex or sensitive processing (see remarks

preliminary), a high level of resources is expected. ". However, it was observed at the beginning

of the survey that the DPO devoted only 50% of his working time to the exercise of his

assignments. The indication that the DPO had the support of an external service provider does not

does not constitute sufficient evidence to demonstrate that the DPO had the resources

sufficient to carry out its duties. The restricted formation therefore rallies

the finding of the head of investigation that the controller was unable to

to demonstrate that it has provided the necessary resources to the DPO for the performance of its tasks.

33.

Finally, if the Restricted Committee has been able to verify that a new DPO has actually been

appointed by the person inspected during the investigation, it nevertheless does not have the

documentation that would verify that it has sufficient resources, and falls under

particular that in his response of August 19, 2020 to the additional letter, the controller

indicated that the DPO performs its tasks at 80%.

34.

In view of the foregoing, the Restricted Committee concludes that Article 38.2 of the GDPR has no

not respected by the controller.

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

1. On the principles

35.

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.

36.

Recital (97) of the GDPR further states that DPOs “should be able

to exercise their functions and missions in full independence”.

37.

According to the DPO Guidelines13, 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

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

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

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

38.

It appears from the audit report that, for the head of investigation to consider objective 7 as completed by the auditee as part of this audit campaign, he expects the DPD is "attached to the highest level of management in order to guarantee its autonomy".

39.

According to the Statement of Objections, page 4, "[i]t appears from the investigation that the DPO is attached to the Director […]. Although formally, in the declaration of appointment, it is planned for the DPO to report directly to the management committee once a quarter, in practice, the reporting of information is done only through the Director of attachment. »

40.

In its position paper of November 14, 2019, the controller argues that the DPD newly appointed is "completely autonomous and reports directly to the level higher in management. He attends the Management Committee and various meetings […]. " The audited further specifies that "[d]regular interviews are scheduled with the members of the Management […] (…)" and that "[d]es recurring interviews on a quarterly basis are planned in a fixed manner to the governance of the Management Committee (annual planning). »

41.

If it does not follow from the provisions of the GDPR that the DPO must necessarily be attached to the highest level of management in order to guarantee its autonomy, the training nevertheless recalls that it noted in point 20 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. »

42.

However, as mentioned in point 21 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 processes a substantial amount of data

whose degree of sensitivity may be relatively high, such as medical data. The

Restricted Committee therefore considers that, in the absence of other measures that would allow

to demonstrate that the DPO is able to directly access the highest level of the

management as soon as he deems it necessary, the reporting line of the DPO to the highest

management level, as expected by the head of investigation, constitutes a proportionate measure

in order to guarantee its autonomy. In this regard, the Restricted Committee notes that at the beginning of

investigation, the DPO of the control was attached to the director […] and not at the highest level of the

direction. It also notes that the auditee does not call into question the precision provided by the

head of inquiry in the statement of objections that although "it is intended that the

DPD reports directly to the management committee once a quarter, in practice the

feedback is only done through the Director to which it is attached. »

43.

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 reports directly to the highest level of management.

44.

In view of the foregoing, the Restricted Committee concludes that Article 38.3 of the GDPR has no

not respected by the controller.

D. On the breach relating to the obligation to ensure that the other missions and tasks of the DPO do not lead to a conflict of interest

1. On the principles

45.

According to Article 38.6 of the GDPR, “[the DPO] may perform other missions and tasks. the responsible for the treatment or the processor ensures that these missions and tasks do not involve a conflict of interest”.

46.

The DPO Guidelines14 specify that “the DPO may not exercise on the within the organization a function that leads it to determine the purposes and means of the processing of personal data”. According to the guidelines, “[i]n good standing general, among the functions likely to give rise to a conflict of interest within organization may include senior management functions (e.g. director general, operational director, director financial, chief medical officer, responsible for marketing department, human resources manager or service manager IT), but also other roles at a lower level of the organizational structure if these functions or roles involve determining the purposes and means of the processing. In addition, there may also be a conflict of interest, for example, if an external DPO is called to represent the data controller or the processor before the courts in cases relating to data protection issues.

Depending on the activities, size and structure of the body, it can be good

practical for data controllers or processors:

 to identify the functions that would be incompatible with those of DPD;

 establish internal rules to this effect, in order to avoid conflicts of interest;

 include a more general explanation regarding conflicts of interest;

 to declare that the DPO has no conflict of interest with regard to his function as

DPD, with the aim of raising awareness of this requirement;

 to provide guarantees in the organization's internal regulations, and to ensure that

that the vacancy notice for the function of DPD or the service contract is

sufficiently precise and detailed to avoid any conflict of interest. In this context, it

should also be kept in mind that conflicts of interest may take

different forms depending on whether the DPO is recruited internally or externally. »

2. In this case

47.

It appears from the audit report that, for the head of investigation to consider objective 5

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

in the event that the DPO performs other functions within the audited body, these functions

do not lead to a conflict of interest, in particular through the exercise of functions that would lead the

DPD to determine the purposes and means of the processing of personal data.

14 WP 243 v.01, version revised and adopted on April 5, 2017, pp.19-20

The head of the investigation also expects the person checked to have carried out an analysis as to

the existence of a possible conflict of interest at DPO level.

48.

According to the statement of objections, page 4, “[i]t appears from the investigation that before being named DPD, the latter was responsible for the IT department. He also exercises, in parallel to its tasks as DPO, the function of […]. If within the framework of its missions of […], the DPO does not participate in […], the fact remains that the latter was involved in the implementation processing of personal data as part of its functions as IT service manager. The DPO could therefore be called upon to decide on processing that he himself implemented as head of the IT department. " Leader investigation further specifies that the person checked "did not know how to bring any element, such as the appointment of an ad hoc DPO to analyze IT processing, allowing to address the risk of conflict of interest. »

49.

In its position paper of November 14, 2019, without questioning the findings made by the head of investigation in the statement of objections, the audit indicates that “[w]ith the appointment of a new full-time DPO, it is ensured that there is no conflicts of interest” and specifies that this new DPO “does not exercise any other function”.

50.

The Restricted Committee notes that the appointment of a new DPO who would not exercise no other function with the controlled, except a support function with the […] for the “contractual management of external parties” (according to the response of the control of the August 19, 2020 to the additional letter), would ensure that the DPO of the controlled does not would not be called upon to comment on the processing for which it would have helped to determine the ends and means.

51.

Nevertheless, the Restricted Committee notes that the designation of the new DPO is intervened during the investigation and therefore agrees with the finding of the head of the investigation, according to

which, at the start of the investigation, the person inspected was unable to demonstrate that there was no conflict interest resulting from the previous functions exercised by the DPO who was then in office.

52.

In view of the foregoing, the Restricted Committee concludes that Article 38.6 of the GDPR has no not respected by the controller.

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

1. On the principles

53.

According to Article 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

54.

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".

55.

On these two points, according to the Statement of Objections, page 5, “[i]t is apparent from
the survey that […], heads of departments as well as members of management have been made aware
to the protection of personal data. The […] then act as a relay for the
outreach to other staff members. Awareness was also
made to the Board of Directors and […]. On the other hand, on the date of the visit of the agents
of the CNPD, the DPD had not participated in any management committee and his participation was not
planned, reporting to the management committee being done via the director […]. Furthermore, he
there is no tool such as an activity report which could have enabled the DPO to address
formal advice to the controller. »

56.

The Restricted Committee finds that the breach noted by the head of investigation does not
concerns that the mission of information and advice of the DPO with regard to the person responsible for the
processing, and not the DPO's task of informing and advising employees.

The Restricted Committee nevertheless takes note of the measures which have been decided by the control
to increase the awareness of its employees, which are described in its policy
of position of 14 November 2019.

57.

With regard to the mission of information and advice with regard to the person in charge of the
treatment, in its position paper of November 14, 2019, the controller indicates that "All

meetings and actions (information, awareness, advice, control, audit, etc.) will be
documented with a view to an activity report for the attention of Management […] and to whom it may concern. »

58.

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.15”

59.

In this respect, it appears from the investigation file that the DPO in office at the time of
the opening of the investigation used the register to verify that the necessary documentation
existed for each processing as well as to identify the processing to be subject to
an impact analysis16.

60.

Nevertheless, the Restricted Committee recalls that it has already noted in point 20 of the
this decision that 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. »

61.

However, as mentioned in point 21 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 processes a substantial amount of data whose degree of sensitivity may be relatively high, such as medical data. The Restricted Committee therefore considers that formal reporting of the DPO's activities to direction, based on a defined frequency, is a proportionate measure to

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

16 Minutes of the visit of 13 February 2019, points 8 and 11

demonstrate that the DPO carries out his duties of information and advice with regard to the controller.

62.

The Restricted Committee takes note of the measures which have been decided in this regard by the controlled, which are described in its position paper of November 14, 2019. Nevertheless, the Restricted Committee notes on the one hand, that the frequency with which the activity reports are addressed to Management […] has not been explained and on the other hand, that these measures have been decided during the investigation. It therefore agrees with the finding of the head of the investigation according to which, at the start of the investigation, the data controller was unable to demonstrate that the DPO carries out his duties of information and advice with regard to the data controller.

63.

The Restricted Committee also notes that it does not have the documentation which would allow him to check the implementation of the measures decided by the control.

64.

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

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

1. On the principles

65.

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.

66.

It follows from the DPO Guidelines17 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;

17 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

67.

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)”.

68.

According to the Statement of Objections, p. 5, “[i]t appears from the investigation that the organization

does not have a formal control plan but a list of tasks, including points

control. In a logic of daily management of data protection, and account-

given the amount of data processed and their sensitivity (see the preliminary remarks), it

it is expected that the control missions of the DPO (…) will be better formalized. »

69.

In its position paper of November 14, 2019, the auditee indicates that the new

DPD has developed and implemented a “…dedicated GDPR” which “includes the register of

treatments and various control points with date of revision of the latter”. Control

specifies that “[t]he DPIA analyzes carried out on the basis of […] are directly attached to the

various treatments. These various actions are recorded in a calendar that is part of

integral to this software. »

70.

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

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.18"

71.

The Restricted Committee has already noted in point 59 of this decision that it is clear

of the investigation file that the DPO in office at the time of the opening of the investigation used the

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

register in order to verify that the necessary documentation existed for each treatment as well as

only to identify the processing operations that must be the subject of an impact assessment19. Training

nevertheless notes that these elements taken in isolation are not sufficient to

allow the controller to demonstrate that the DPO can carry out its mission of control of the

adequate compliance with the GDPR.

72.

The Restricted Committee recalls that it has noted in point 20 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. »

73.

However, as mentioned in point 21 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 processes a substantial amount of data

whose degree of sensitivity may be relatively high, such as medical data.

74.

The Restricted Committee therefore considers that the inspection mission carried out

by the DPO to the auditee should be sufficiently formalized, for example by a plan

of data protection control, in order to allow the controlled to demonstrate

that the DPO can carry out its task of monitoring compliance with the GDPR in an adequate manner.

75.

However, the Restricted Committee notes that it appears from the investigation file and the elements

communicated by the audited in its position paper of November 14, 2019 that the mission

control carried out by the DPO was not sufficiently formalized at the time of the opening

of the investigation.

76.

The Restricted Committee takes note of the fact that in its letter of 19 August 2020, the

controlled indicates that the new DPO “has already had various internal procedures modified in order to

that the protection of personal data is well taken into account within our

various activities” and that a “follow-up plan for our various treatments, according to their

sensitivities, has (…) been put in place. »

77.

Nevertheless, the Restricted Committee observes that these measures were decided in

investigation and therefore agrees with the finding of the head of investigation that, at the

19 Minutes of the visit of 13 February 2019, points 8 and 11

---

start of the investigation, the auditee was unable to demonstrate that the DPO exercises its missions to monitor compliance with the GDPR in a manner adapted to its needs.

78.

The Restricted Committee also notes that it does not have the documentation which would make it possible to demonstrate that the measures mentioned in point 76 of this Decision were put in place by the controller.

79.

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

III.

On the corrective measures and the fine

A. Principles

80. 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. »

81. Article 83 of the GDPR provides that each supervisory authority shall ensure that fines

administrative measures imposed are, in each case, effective, proportionate and

deterrents, before specifying the elements that must be taken into account to decide

whether an administrative fine should be imposed and to decide on the amount of this

fine :

(a) the nature, gravity and duration of the breach, taking into account the nature, scope or

the purpose of the processing concerned, as well as the number of data subjects

affected and the level of damage they suffered;

b) whether the breach was committed willfully or negligently;

c) any action taken by the controller or processor to mitigate the

damage suffered by the persons concerned;

d) the degree of responsibility of the controller or processor, account

given the technical and organizational measures they have implemented under the

sections 25 and 32;

---

e) any relevant breach previously committed by the controller or

the subcontractor ;

f) the degree of cooperation established with the supervisory authority with a view to remedying the breach

and to mitigate any negative effects;

g) the categories of personal data affected by the breach;

h) the manner in which the supervisory authority became aware of the breach, in particular whether,

and the extent to which the controller or processor notified the

breach ;

(i) where measures referred to in Article 58(2) have previously been

ordered against the controller or processor concerned for the

same purpose, compliance with these measures;

(j) the application of codes of conduct approved pursuant to Article 40 or

certification mechanisms approved under Article 42; and

k) any other aggravating or mitigating circumstance applicable to the circumstances of

the species, such as the financial advantages obtained or the losses avoided, directly or

indirectly, as a result of the breach".

82.

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. Possible changes

relating to the subject of the investigation that took place subsequently, even if they make it possible to establish

full or partial compliance, do not permit the retroactive cancellation of a

breach found.

83.

Nevertheless, the steps taken by the control to bring itself into compliance

with the GDPR during the investigation process or to remedy breaches

raised by the head of investigation in the statement of objections are taken into account by the

restricted training in the context of any corrective measures and/or the setting of the

amount of any administrative fine to be imposed.

B. In the instant case

1. Regarding the imposition of an administrative fine

84.

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

head of investigation proposes to the restricted committee to pronounce against the person controlled a

administrative fine in the amount of 17,700 euros.

85.

In order to decide whether to impose an administrative fine and to decide, if

applicable, of the amount of this fine, the Restricted Committee analyzes the criteria laid down by

GDPR Article 83.2:

- As to the nature and gravity of the breach [Article 83.2 a) of the GDPR], with regard to

breaches of Articles 37.5, 38.2, 38.3, 38.6, 39.1.a) and 39.1.b) of the GDPR, training

restricted notes that the appointment of a DPO by an organization cannot be efficient and

effective, namely facilitating compliance with the GDPR by the organization, only in the event that the DPO

has sufficient professional qualities and the necessary resources to

the exercise of its missions, exercises its functions and missions in complete independence, does not exercise

no other duties that could lead to a conflict of interest, exercises effectively

its missions, including the mission of informing and advising the controller and the

GDPR compliance monitoring mission.

- As for the duration criterion [article 83.2.a) of the GDPR], the restricted training falls under:

(1) That a new DPO, with sufficient expertise in data protection

data, was hired and appointed by the controller on November 13, 2019.

The breach of Article 37.5 of the GDPR therefore lasted over time, between May 25

2018 and November 13, 2019;

(2) That it has not been demonstrated by the controller that the DPO in office at the time of

the opening of the investigation had the necessary resources for the exercise of its

missions and that according to the letter of the control of August 19, 2020, the new DPD "carries out his mission (…) over a period of 80% of his time. The remaining 20% consist of assisting the […] in contract management with external stakeholders ". The breach of Article 38.2 of the GDPR therefore lasted over time, from 25 May 2018, it being specified that the Restricted Committee was unable to ascertain that the breach has ended;

---

(3) That it has not been demonstrated by the controller that the DPO in office at the time of the opening of the investigation could directly access the highest level of management whenever he deemed it necessary. This has also not been demonstrated for the new DPD. The breach of Article 38.3 of the GDPR therefore lasted over time, from May 25, 2018, it being specified that the Restricted Committee was unable to ascertain that the breach has ended;

(4) That the new DPO, hired and appointed by the control on November 13 2019, does not exercise any other function with the controlled, except, according to the mail of the audit of August 19, 2020, a support function with […] for the "management contract of external parties". The breach of Article 38.6 of the GDPR has therefore lasted over time, between May 25, 2018 and November 13, 2019;

(5) That in his letter of August 19, 2020, the controller indicates that the new DPD "has already had various internal procedures modified so that data protection of a personal nature is taken into account in our various activities" and that a "monitoring plan for our various treatments, depending on their sensitivities, has (…) been put in place". The breach of Article 39.1.b) of the GDPR therefore lasted for the

time, at least between May 25, 2018 and August 19, 2020;

(6) That it has not been demonstrated by the controller that the DPO in office at the time of the opening of the investigation exercised its missions of information and advice with regard to the data controller, and that, in its position paper of November 14, 2019, the frequency with which the established activity reports are sent to Management […] has not not explained by the controller. The breach of Article 39.1.a) of the GDPR therefore lasted in time, at least between May 25, 2018 and November 14, 2019.

- As for the degree of cooperation established with the supervisory authority [article 83.2 f) of the GDPR], the restricted training takes into account the assertion of the head of investigation that the control has demonstrates constructive participation throughout the investigation.

- As to the categories of personal data concerned by the breach [Article 83.2 g) of the GDPR], the restricted training takes into account the fact that the audit deals with special categories of personal data, in particular data concerning health.

86.

The Restricted Committee notes that the other criteria of Article 83.2 of the GDPR do not are neither relevant nor likely to influence its decision on the imposition of a fine administrative and its amount.

87.

The Restricted Committee notes that if several measures have been decided by the control in order to remedy in whole or in part certain shortcomings, these have only been decided that following the launch of the investigation by CNPD agents on September 17

2018 (see also point 82 of this decision).

88.

Therefore, the Restricted Committee considers that the imposition of a fine
administrative is justified with regard to the criteria laid down by article 83.2 of the GDPR for
breach of Articles 37.5, 38.2, 38.3, 38.6, 39.1.a) and 39.1.b) of the GDPR.

89.

With regard to the amount of the administrative fine, the Restricted Committee recalls that
Article 83.3 of the GDPR provides that in the event of multiple infringements, as is the case in
case, the total amount of the fine may not exceed the amount set for the most serious violation.
severe. To the extent that a breach of Articles 37.5, 38.2, 38.3, 38.6, 39.1.a) and 39.1.b)
of the GDPR is reproached to the controlled, the maximum amount of the fine that can be retained
amounts to 10 million euros or 2% of worldwide annual turnover, whichever is greater
high being retained.

90.

With regard to the relevant criteria of Article 83.2 of the GDPR mentioned above, the
Restricted Committee considers that the pronouncement of a fine of 10,700 euros appears
effective, proportionate and dissuasive, in accordance with the requirements of Article 83.1 of the GDPR.

2. Regarding the taking of corrective measures

91.

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 team "
Data Protection "dedicated) to acquire sufficient expertise adapted to the needs
of the data controller in terms of data protection 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 envisaged to achieve this result, one of the possibilities could be
to appoint another DPO who has sufficient expertise. Several measures
such as those listed below can be considered to achieve this
results:

- provide formal internal or external support to your DPO in matters of data protection
data and information systems;
- enroll your DPO in / continue accelerated/intensive training in
data protection and information systems;
- designate another DPO who has sufficient expertise.

b) Order the provision of necessary resources to the DPO in accordance with
the requirements of Article 38 paragraph 2 of the GDPR. Although several ways
could be envisaged to achieve this result, one of the possibilities could be
to relieve the DPO of all or part of his other missions/functions and/or of him
provide formal support, internally or externally, for the exercise of its missions
from DPD.

c) Order the effective deployment of a mechanism guaranteeing the autonomy of the DPO
in accordance with the requirements of Article 38 paragraph 3 of the GDPR. The DPO must
able to intervene personally at the highest level of the hierarchy. Although
several ways can be envisaged to achieve this result, one of the

possibilities could be to ensure that the DPO in particular directly attends the

Management Committee and various project meetings.

d) Order the deployment of measures ensuring that the various missions and tasks

of the person exercising the function of DPO do not lead to conflicts of interest

in accordance with the requirements of Article 38 paragraph 6 of the GDPR. Although several

ways can be envisaged to achieve this result, one of the possibilities

would be the involvement of a third party, benefiting from the necessary skills,

for the review of treatments for which there is a conflict of interest, namely the

IT treatments. Another possibility would be to designate a DPO who is not brought

to decide on the treatments that he himself has put in place.

---

e) Order the deployment of the control mission, in accordance with article 39

paragraph 1 b) of the GDPR. Although several ways can be envisaged to

achieve this result, the DPO should document its controls on the application of

internal data protection rules and procedures (second line

defence). This documentation could take the form of a control plan. »

92. As for the corrective measures proposed by the head of investigation and with reference to point

83 of this decision, the Restricted Committee takes into account the steps

carried out by the controlled in order to comply with the provisions of Articles 37.5, 38.2,

38.3, 38.6 and 39.1.b) of the GDPR, in particular the measures described in its letter of 19

August 2020. More specifically, it notes the following facts:

- With regard to the violation of Article 37.5 of the GDPR, the Restricted Committee finds

that the auditee has appointed a new DPO with expertise

sufficient. The Restricted Committee therefore considers that there is no need to pronounce the corrective measure proposed by the head of investigation and repeated under a) of point 91 of the this decision.

- With regard to the violation of Article 38.2 of the GDPR, the controller indicates in its letter of August 19, 2020 that the new DPO "performs its mission (…) over a period 80% of his time. The remaining 20% consists of assisting the […] in the management contract with external parties. Given the fact that the audit deals a substantial amount of data whose degree of sensitivity may be relatively high, the Restricted Committee considers that the DPO should have more resources for the performance of its duties. The Restricted Committee therefore considers that there is reason to pronounce the corrective measure proposed by the head of investigation and repeated under b) of point 91 of this decision.

- With regard to the violation of Article 38.3, the Restricted Panel finds that the elements communicated by the controller in his letter of August 19, 2020 are not sufficient to demonstrate that the DPO is able to directly access the highest level of the management whenever he deems it necessary. The Restricted Committee therefore considers that there is place to pronounce the corrective measure proposed by the head of investigation and included under c) of point 91 of this Decision.

- With regard to the violation of Article 38.6, the Restricted Committee considers that the appointment of a new DPO who does not exercise any other function with the auditee, if this is, according to the audit letter of August 19, 2020, a support function with […] for the "contractual management of external stakeholders", makes it possible to ensure that the

DPD will not be called upon to comment on the processing of which it would have contributed to determine the ends and the means. The Restricted Committee therefore considers that there is no no need to pronounce the corrective measure proposed by the head of investigation and resumed under (d) point 91 of this decision.

- With regard to the violation of Article 39.1.b) of the GDPR, the restricted training takes notes that in his letter of August 19, 2020, the controller indicates that the new DPD “has already had various internal procedures modified so that the protection of personal data is properly taken into account within our various activities” and that a “follow-up plan for our various treatments, according to their sensitivities, has (…) been put in place”. Nevertheless, the restricted formation does not have documentation to demonstrate the implementation of these measures. The Restricted Committee therefore considers that it is appropriate to pronounce the corrective measure proposed by the head of investigation and reproduced under e) of point 91 of this decision.

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, 38.2, 38.3, 38.6, 39.1.a) and 39.1.b) of the GDPR;
- to impose an administrative fine on “Foundation A” in the amount of ten thousand seven hundred euros (10,700 euros) with regard to the violation of articles 37.5, 38.2, 38.3, 38.6, 39.1.a) and 39.1.b) GDPR;
- to pronounce against "Foundation A", an injunction to comply with Article 38.2 of the GDPR, within four months of notification of the decision restricted training, in particular:

ensure that the DPO has the necessary resources to carry out his duties;

- to pronounce against "Foundation A", an injunction to comply

with Article 38.3 of the GDPR, within four months of notification of the decision

restricted training, in particular:

ensure the establishment and maintenance of a formal mechanism guaranteeing the autonomy

the DPO;

- to pronounce against "Foundation 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, in particular:

ensure the formal and documented deployment of the DPO's control mission.

Thus decided in Belvaux on August 4, 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.

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

survey no.[…] conducted with “Foundation A”