Decision of the National Commission sitting in restricted formation on

the outcome of survey no. […] conducted with Company A

Deliberation No. 40FR/2021 of October 27, 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 on the

protection of natural persons with regard to the processing of 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 of

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 10.2;

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

investigation 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 (Regulation general on data protection) (hereinafter: the "GDPR"), the National Commission for the 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 and public sectors.

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 the Company A, established at L-[…], […], and registered in the trade and companies register under number […] (hereinafter, the "controlled") and to designate Mr. Christophe Buschmann as head of investigation. Said deliberation specifies that the investigation relates to the conformity of the control with the section 4 of chapter 4 of the GDPR.

3.

The corporate purpose of the audited company is the operation of a transport company […].2 In 2018, the audited had about […] employees and provided its services to about […] [people] per year.3

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

4.

preliminary to the audit, to which the latter responded by letter dated October 1, 2018. A visit on site took place on February 20, 2019. Following these exchanges, the head of investigation drew up the report audit report No […] (hereinafter: the "audit report").

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.

2 Corporate purpose as declared in the Luxembourg Trade and Companies Register, article 2.1 of the articles of association coordinated with the […] of the controlled.

3 Report of the on-site visit of February 20, 2019.

It appears from the audit report that in order to verify compliance of the audit with section 4 5.

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

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 effectively carry out its his 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 the processing of data within 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 30, 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

identified during his investigation. The audit report was attached to the said letter of October 30, 2019.

7.

In particular, the head of investigation noted in the statement of objections

breaches of:

the obligation to involve the DPO in all questions relating to data protection

-

of a personal nature4;

4 Objective 8

-

-

-

the obligation to guarantee the autonomy of the DPO5;

the information and advisory missions of the DPO6;

the control mission of the DPD7.

8.

On August 3, 2020, the head of investigation sent an additional letter to the controller to the

statement of objections (hereinafter: the “additional letter to the statement of

grievances") by which he informs the control of the corrective measures that the head of investigation proposes to the National Commission sitting in restricted formation (hereinafter: the "restricted formation") to adopt.

9.

By letters dated December 12, 2019 and October 14, 2020, the controller sent the chief of inquiry its position on the statement of objections and the additional letter to the statement of objections. In these letters, the controller presents his observations relating to each shortcoming raised by the head of investigation in the statement of objections and disputes the proposal for an administrative fine, "the breaches described falling more of formalism than of a non-execution of the roles and missions of the DPO".

10.

The president of the restricted formation informed the control by letter of April 12, 2021 that his case would be registered for the session of the Restricted Committee on June 16, 2021 and that he could attend this session. The controlled informed by email of May 12, 2021 that he would participate in said session.

11.

During the restricted training session of June 16, 2021, the head of investigation and the controlled presented their oral observations on the case and answered the questions posed by restricted formation. The controller spoke last.

12.

The controller provided additional information by letter dated June 29, 2021, following to a request in this sense from the restricted formation.

5 Objective 7

6 Objective 9

7 Goal 10

II.

Place

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

1. On the principles

13.

According to Article 38.1 of the GDPR, the organization must ensure that the DPO is associated, on a in a timely and appropriate manner to all questions relating to data protection of a personal nature.

14.

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. [...] Informing and consulting the DPO from the outset will allow to facilitate compliance with the GDPR and to encourage an approach based on the protection of data by design; it should therefore be standard procedure within the governance of the organization. Furthermore, it is important that the DPO be considered as a interlocutor within the organization and that he is a member of the working groups devoted to data processing activities within the organisation”8.

The DPO Guidelines provide examples on how

15.

to ensure this association of the DPO, such as:

- invite the DPO to regularly participate in senior management meetings and

intermediate ;

-

recommend the presence of the DPO when decisions having implications in

data protection matters are taken;

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

-

immediately consult the DPO when a data breach or other incident occurs

product.

8 WP 243 v.01, version revised and adopted on April 5, 2017, page 16

16.

In addition, according to the DPO guidelines, the organization could, if necessary

where appropriate, develop guidelines or programs for the protection of

data indicating the processing operations in which the DPO must be consulted.

2. In this case

17.

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

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

participates in a formalized manner and on the basis of a defined frequency in the Management Committee,

project coordination committees, new product committees, safety committees or

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

18.

According to the statement of objections, page 2, the DPO of control participates in the Committee of

Management according to the agenda (in this case to the Management Committees of May 30 2018, August 1, 2018 and February 5, 2019) as well as project management meetings. No rules or frequency has been formally defined as to the participation of the DPO in these committees or meetings.

19. In its position paper of December 12, 2019, the auditee indicated that, from the 1st January 2020, a quarterly activity report on the protection of personal data will be presented to the Management Committee within 2 weeks of the end of each quarter considered.

20. In its position paper of October 14, 2020, the auditee added that, since the Appointment of the DPO on May 15, 2018, he participates in Management Committees on a regular basis. In addition, the DPO's activity reports were presented to the Management Committee on 6 occasions between May 2018 and December 2019, i.e. a quarterly frequency. This frequency of presentation of the activity report was formalized as indicated in the letter of 12 December 2019. According to the auditee, this is therefore a simple formalization of a practice already in square.

21. In addition, the control indicates that the DPO can be consulted ad hoc, by the Committee of Management as soon as a question relating to the processing of personal data arises.

"This possibility has been activated several times over the past two years (2018-2020) and especially in recent months as part of the measures put in place in the fight against

Covid-19: the DPO notably participated in the Management Committees of July 21, 2020 and July 22 September 2020".

The controller also explains that the DPD is associated with the design of new

22.

projects and the implementation of new IT solutions as follows:

the DPO is contacted systematically as soon as a new project or product is launched.

-

"The project methodology indeed imposes a stage of analysis and validation between the DPO and the department initiating or managing the new idea to be implemented".

- "In case of selection of an external service provider for the selection of a new IT solution or to outsource a data management process (regardless of the type of data exchanged), the DPO is a stakeholder in the evaluation of the service provider concerned. »
- "The project portfolio management meetings [of the auditee] are held on a monthly basis and the DPD is a systematically present function not only to take notice of new ideas that may emerge in different departments before they become projects. This step allows you to potentially alert on the compliance risks to be taken into account very early in the initiatives. »

23.

In his letter of June 29, 2021, the controller also informs the restricted training that the DPO must approve each request relating to a transfer of personal data to local and foreign authorities, in accordance with the personal data transfer policy to local and foreign authorities set up in May 2018.

24.

The Restricted Committee takes note of the implementation by the control of a formalization

the involvement of the DPO with the Management Committee. If this formalization measure should facilitate the involvement of the DPO in all matters relating to data protection, it should nevertheless be noted that this was decided during the investigation.

25.

In addition, the auditee did not provide evidence as to the presentation of the report activities of the DPO to the Management Committee on a quarterly basis between May 2018 and December 2019. Indeed, in its position paper of October 14, 2020, the auditee maintains that a activity report is presented to the Management Committee on a quarterly basis but,

With regard to the documents sent in the appendix to this letter, the controller only provides proof for the presentation made to the Management Committee in December 2019.

The Restricted Committee therefore agrees with the finding of the head of investigation that,

26.

at the start of the investigation, the controller was unable to demonstrate that the DPD was appropriately involved in all questions relating to the protection of personal data.

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

27.

not been respected.

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

1. On the principles

28.

Under Article 38.3 of the GDPR, the organization must ensure that the DPO “receives no

no instructions with regard to the exercise of the missions". Furthermore, the DPD "does

report directly to the highest level of management" of the organization.

29.

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

to exercise their functions and missions in complete independence".

According to the DPO Guidelines9, Article 38.3 of the GDPR "provides

30.

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 deal with a case, for example, what result should be obtained,

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

how to investigate a complaint or whether to consult the supervisory authority. In addition, they

cannot be required to adopt a certain point of view on a matter relating to the legislation in question.

data protection, for example, a particular interpretation of the 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 clearly indicate his opinion

diverge at the highest level of management and decision makers. In this regard, Article 38,

paragraph 3, provides that the DPO "reports directly to the highest level of the

direction of the controller or processor". Such direct accountability

ensures that senior management (e.g. the board of directors) is aware of the

opinions and recommendations of the DPO which fall within the scope of the latter's mission

consisting of informing and advising the controller or processor. The development

an annual report on the activities of the DPO for the highest level of management

is another example of direct accountability. »

2. In this case

31.

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

completed by the controller as part of this audit campaign, he expects the DPO to be

“attached to the highest level of management in order to guarantee its autonomy as much as possible”.

32.

According to the statement of objections, page 3, “[d]uring the investigation, CNPD officials

noted that the DPO reports hierarchically to the “Risk Management and

Internal Audit ". This department is attached to the General Services, which themselves depend

of the Directorate. There are therefore two hierarchical levels between the DPO and the Management. Although the

DPD is functionally attached to the Management and participates in the Management Committee in

depending on the agenda, the hierarchical attachment to Management and therefore direct and

permanent to the latter is not formally guaranteed. »

In its position papers of December 12, 2019 and October 14, 2020, the auditee indicates

33.

that “[t]he guarantee of the DPO’s autonomy, and direct access to General Management, which were

already a practical reality at the time of [the] audit, have been reinforced and materialized in

the organization chart of the company. The DPO now reports directly to the Directorate of

General Services, and no longer in the Risk Management and Internal Audit department. » A new

organizational chart was published on December 11, 2019 to reflect this change.

As regards the hierarchical attachment, if it does not result from the provisions of the GDPR

34.

that the DPO must necessarily be attached to the highest level of management in order to

guarantee its autonomy, the Restricted Committee nevertheless notes that it is rightly specified in

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”.

However, the Restricted Committee shares the assessment of the Head of Investigation, mentioned on page

35.

2 of the statement of objections, according to which the auditee “processes (...) a significant number of

personal data ".

The Restricted Committee considers that the audit did not demonstrate the implementation

36.

other measures that would demonstrate that the DPO is able to access

directly to the highest level of management as soon as he deems it necessary, without having to

necessarily pass through the intermediate hierarchical levels. Therefore, the connection

hierarchy of the DPO at the highest level of management, according to the expectations of the head of investigation,

constitutes a proportionate measure in order to guarantee its autonomy. In this regard, training

restricted notes that the reporting of the DPO to the highest level of management has not been decided

by the controller only after the start of the investigation.

In view of the foregoing, the Restricted Committee agrees with the finding of the head of investigation

37.

that, at the start of the investigation, the controller was unable to

demonstrate that the DPO could act without receiving instructions with regard to the exercise of

his missions.

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

38.

not respected by the controller.

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

1. On the principles

39.

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

40.

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

completed by the controller as part of this audit campaign, the head of investigation expects that

that “the organization has formal reporting of the activities of the DPO to the Management Committee

based on a defined frequency. Regarding information to employees, it is expected that

the organization has put in place an adequate staff training system in terms of

Data protection ".

41.

According to the statement of objections, page 3, “[i]t appears from the investigation that the body did not
no specific activity reporting on data protection intended for management
superior (Executive Committee, Board of Directors). Although regular points are
made to the Management Committee on issues related to data protection
and that all procedures relating to data protection are submitted to the Management
for validation, these elements cannot compensate for the absence of formal reporting of activities
from the DPO to the Management Committee on the basis of a defined frequency”.

In its position paper of December 12, 2019, the controller states that the DPD

42.

“carries out regular updates to the Management Committee on its activity, without the periodicity of
this reporting has been formally defined. From January 1, 2020, a quarterly report
activity in terms of data protection will be presented to the Management Committee, within the
2 weeks following the end of each considered quarter. »

43.

In its position paper of October 14, 2020, the auditee also indicates that "[t]he
notion of regular reporting to General Management was already present in
the amendment of the DPO contract, on a bi-annual basis. This reporting frequency has been
raised and increased to 4 times a year”. This amendment to the DPO contract was however signed on 31
March 2020, i.e. after the start of the investigation.

The Restricted Committee notes that Article 39.1 of the GDPR lists the missions that the

44.

DPD must at least be entrusted with the task of informing and advising the organization as well as

than employees, without however specifying whether specific measures must be put in place to ensure that the DPO can fulfill his mission of information and advice. The lines guidelines on DPOs, which provide recommendations and best practices to guide data controllers in achieving compliance with their governance, also only briefly address the mission of advising and informing the DPD. Thus, they specify 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 tasks of monitoring compliance with the GDPR as well as information and advice from the controller or processor".

45. It appears from the investigation file that the DPO submits regular points relating to the data protection to the Management Committee. The DPD for example presented in February 2019 monitoring of GDPR compliance as of December 31, 2018 and, in August 2018, a study on the consent and the issue of data retention. However, there is no specific activity reporting, based on a defined frequency.10

46. Nevertheless, the Restricted Committee recalls that it has already noted in point 34 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 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".

10 Visit report of February 20, 2019, p. 4, and audit report, p.8

47.

However, as mentioned in point 35 of this decision, the restricted committee
shares the assessment of the head of investigation, mentioned on page 2 of the statement of objections,
that the controlled "processes (...) a significant amount of personal data". The
Restricted Committee therefore considers that formal reporting of the DPO's activities to the
direction, based on a defined frequency, constitutes a proportionate measure in order to
demonstrate that the DPO carries out his missions of information and advice with regard to the person in charge
of the treatment.

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

48.

December 12, 2019 and October 14, 2020 that it was decided to set up formal reporting
DPO activities on a quarterly basis. The restricted formation, which does not have the
documentation which would make it possible to demonstrate the implementation of this measure, notes that
this was decided during the investigation and therefore agrees with the finding of the head of the investigation
that, at the start of the investigation, the controller was unable to
demonstrate that the DPO carries out his missions of information and advice with regard to the person in charge
of the treatment.

In view of the foregoing, the Restricted Committee concludes that Article 39.1 a) of the GDPR has no

49.

not respected by the controller.

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

1. On the principles

50.

According to Article 39.1 b) of the GDPR, the DPO has, among other things, the mission of “monitoring compliance
of this Regulation, other provisions of Union law or the law of the Member States in

data protection and the internal rules of the controller or the

subcontractor with regard to the protection of personal data, including with regard to

concerns the distribution of responsibilities, awareness and training of staff

involved in processing operations, and related audits".

51.

Recital (97) clarifies that the DPO should assist the organization in verifying compliance, at

internal level, of the GDPR.

52.

It follows from the DPO Guidelines11 that the DPO may, in the context of

these control tasks, in particular:

collect information to identify processing activities;

-

- analyze and verify the compliance of processing activities;

-

inform and advise the controller or processor and formulate

recommendations to him.

2. In this case

53.

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 formal data protection control plan

(even if it is not yet executed).

54.

According to the statement of objections, page 3, “[i]t appears from the investigation that the body does not

does not have a formal control plan specific to data protection. The CNPD

notes that an annual data protection review is provided for by the

legal department as well as a regular review of the processing register. The CNPD notes

also that a Compliance Officer who will have in his attributions the regular review of the

data protection compliance is being recruited and assignments

data protection controls will be included in the internal audit plan.

However, the organization was not carrying out control missions at the time of the survey. »

In its position paper of December 12, 2019, the control indicates that a Compliance

55.

Officer directly attached to the General Services Department has been appointed, with in his

responsibilities the regular review of data protection compliance.

In its position paper of October 14, 2020, the auditee presents the controls that have

56.

been carried out and documented by the DPO:

11 WP 243 v.01, version revised and adopted on April 5, 2017, page 20

- For each new project and product, the DPO reviews the process, documents the level

risks and reviews the contractual documents in collaboration with the legal department.

- A contractual review is carried out annually with the legal department

since the creation of the DPO function.

- A project to audit data retention procedures was carried out in

2019 with the help of an external consultant under the supervision of the DPO. The conclusions of this study were presented during the DPO's activity report in December 2019.

- The DPO has taken on ad-hoc checks on several occasions following requests information of data subjects.
- In December 2019, the control appointed its auditor to conduct a review of “Data Protection Office” procedures and controls in place to assess the associated GDPR risks. The DPO was involved in this review.

57.

In his letter of June 29, 2021, the controller adds that […] “Data Protection Coordinators” were appointed in May 2018 to monitor the compliance of practices with the requirements of the GDPR and report to the DPO. These Data Protection Coordinators received training in June and July 2018 as well as in February and March 2021.

58.

The control also indicates the establishment of biannual meetings between the DPO and the Director General to discuss upcoming control projects. These biannual meetings are mentioned in the addendum to the DPO contract signed on March 31, 2020, as mentioned in point 43 of this decision.

59.

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 monitoring compliance with the GDPR, without however require the organization to put in place specific measures to ensure that the DPO can accomplish its mission of control. The DPO guidelines indicate in particular that the maintenance of the register of processing activities referred to in Article 30 of the GDPR may be entrusted to the DPO and that “this register should be considered as one of the tools allowing the DPO

survey no.[…] conducted with Company A

15/26

to carry out its missions of monitoring compliance with the GDPR, as well as informing and advising the controller and processor12".

60.

In addition, the Restricted Committee recalls that it has already noted in point 34 of this decision that it is rightly stated on page 2 of the statement of objections (under "remarks preliminary") that "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".

61.

However, as mentioned in point 35 of this decision, the Restricted Committee shares the assessment of the head of investigation, mentioned on page 2 of the statement of objections, according to which the controller processes a significant amount of personal data.

The Restricted Committee understands that the controller has implemented several measures to

62.

to strengthen the capacities of the DPO to carry out its mission of monitoring compliance with the GDPR, such as that the appointment of a Compliance Officer and the setting up of biannual meetings between the DPD and the Managing Director. However, these measures were taken during the investigation.

Given the fact that the activities of the controller involve the processing of data

63.

of a personal nature which affect a large number of data subjects, the training restricted considers that the control mission carried out by the DPO with the controlled party must be formalised, for example by a data protection control plan, in order to be able to demonstrate that the DPO can carry out its mission of monitoring compliance with the GDPR by

adequate way.

Consequently, the Restricted Committee is of the opinion that the controlled was not able

64.

to demonstrate that, at the start of the investigation, the DPO could exercise his mission of monitoring the

compliance of the data controller with the GDPR.

12 WP 243 v.01, version revised and adopted on April 5, 2017, page 22

65.

In view of the foregoing, the Restricted Committee concludes that Article 39.1 b) of the GDPR has no

not respected by the controller.

III.

On the corrective measures and the fine

A. Principles

66.

In accordance with article 12 of the law of August 1, 2018 on the organization of the

National Commission for Data Protection and the general data protection regime

data, the National Commission has the powers provided for in Article 58.2 of the GDPR:

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

envisaged processing operations are likely to violate the provisions

of these regulations;

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

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

regulation;

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

requests made by the data subject to exercise their rights in

application of this regulation;

(d) order the controller or processor to put the

processing operations in accordance with the provisions of this Regulation,

where applicable, in a specific manner and within a specified period;

(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 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 direct the certification body to withdraw a

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

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

specific characteristics of each case;

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

a third country or an international organisation. »

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

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

before specifying the elements that must be taken into account to decide whether to impose

an administrative fine and to decide on the amount of this fine:

(a) “the nature, gravity and duration of the violation, taking into account the nature,

scope or purpose of the processing concerned, as well as the number of persons

concerned affected and the level of damage they have 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,

given the technical and organizational measures they have put in place

works under Articles 25 and 32;

e) any relevant violation previously committed by the person in charge of the

processor or processor;

f)

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

violation and to mitigate any adverse effects;

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

h) how the supervisory authority became aware of the breach, including

whether, and to what extent, the controller or processor has notified

the violation ;

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 case, such as the financial advantages obtained or the losses avoided,

directly or indirectly, by reason of the breach".

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

68.

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.

69.

Nevertheless, the steps taken by the controller to comply with

the GDPR during the investigation procedure or to remedy the breaches identified by the head of investigation in the statement of objections are taken into account by the restricted committee within the framework of any corrective measures and/or the fixing of the amount of a possible administrative fine to be pronounced.

B. In the instant case

1. Regarding the imposition of an administrative fine

70.

In his supplementary letter to the statement of objections of 3 August 2020, the head of investigation proposes to the restricted formation to pronounce against the controlled a fine administrative relating to the amount of 15,400 euros.

71.

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 38.1, 38.3, 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 to facilitate compliance with the GDPR by the organization, only in the event that the DPD is associated with all questions relating to data protection, whether carry out its function in complete autonomy, and can effectively carry out its missions, including the task of informing and advising the data controller and the task of monitoring compliance with the GDPR.

- As for the duration criterion [article 83.2 a) of the GDPR], the Restricted Committee notes that:

(1) The controller informed the CNPD, in its position papers of December 12, 2019, October 14, 2020 and June 21, 2021, from the formalization of the DPO's association with data protection issues. These measures have nevertheless been

decided during the investigation. For example, according to the information available restricted training, the formalization of the reporting of the activities of the DPO on a quarterly frequency would have been put in place on January 1, 2020 (taking position of the audit of December 12, 2019) whereas, in the amendment to the contract of DPD signed on March 31, 2020 (appended to the control position paper of October 14 2020), the frequency of reporting is mentioned as biannual. the breach of Article 38.1 of the GDPR therefore lasted over time, at least for May 25, 2018 to January 1, 2020.

(2) In its position papers of December 12, 2019 and October 14, 2020, the auditee informed the CNPD of a change in the organization chart of the organization, published on 11 December 2019, so that the DPO is now attached directly to the Department of General Services. The breach of Article 38.3 of the GDPR therefore lasted in time, at least from May 25, 2018 to December 11, 2019.

(3) It has not been demonstrated by the person audited that, at the time of the opening of the investigation, the DPD carried out its missions of information and advice with regard to the manager of the treatment. As noted in point (1) above and in point 48 of this decision, reporting of DPO activities on a quarterly basis would have been implemented on January 1, 2020, while in the amendment to the contract of work of the DPO signed on March 31, 2020, the frequency of reporting is mentioned as biannual. The restricted training therefore includes that reporting by the DPD at the control department has been put in place, although the frequency of this reporting is not clarified. The breach of Article 39.1(a) therefore lasted for the

time, at least from May 25, 2018 to January 1, 2020.

(4) It has not been demonstrated that the DPO fulfills its mission of monitoring compliance with the GDPR by the controller at the start of the investigation. The controller informed the CNPD of the appointment of a Compliance Officer in charge of this control, without however indicating the date of this appointment. In addition, the controller indicated the implementation of bi-annual meetings between the DPO and the Director General, as foreseen in the amendment to the DPO contract signed on March 31, 2020 and already mentioned in points 43

and 58 of this decision. These measures were nevertheless decided on during of investigation and the restricted formation does not have the necessary documentation showing that the breach has ended. Breach of Section 39.1 b) of the GDPR therefore lasted in time, from May 25, 2018.

- As for the criterion to be taken into account relating to the number of persons concerned, if any, affected by the breach and the level of damage, if any, suffered [article 83.2 a) of the GDPR], the Restricted Committee notes that the audited counts approximately […] employees and […] of [people] per year.
- As to the degree of cooperation established with the supervisory authority [Article 83.2 f) of the GDPR], the restricted formation takes into account the assertion of the head of investigation that the auditee demonstrated constructive participation throughout the investigation.

72.

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

73.

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 were only decided upon following the launch of the investigation by CNPD agents on September 17, 2018 (see also point 68 of this decision).

Therefore, the Restricted Committee considers that the pronouncement of an administrative fine

74.

is justified with regard to the criteria set out in article 83.2 of the GDPR for breaches of articles 38.1, 38.3, 39.1 a) and 39.1 b) GDPR.

With regard to the amount of the administrative fine, the Restricted Committee recalls that

75.

Article 83.3 of the GDPR provides that in the event of multiple infringements, as is the case here, the total amount of the fine cannot exceed the amount fixed for the most serious violation. In the extent to which a violation of Articles 38.1, 38.3, 39.1 a) and 39.1 b) of the GDPR is alleged at the time of the audit, the maximum amount of the fine that can be withheld is 10 million euros or 2% of annual worldwide revenue, whichever is greater.

With regard to the relevant criteria of Article 83.2 of the GDPR mentioned above, the training

76.

Restricted considers that the imposition of a fine of 15,400 euros appears to be both effective, proportionate and dissuasive, in accordance with the requirements of Article 83.1 of the GDPR.

2. Regarding the taking of corrective measures

77.

In his supplementary letter to the statement of objections of 3 August 2020, the head of investigation proposes to the Restricted Committee to take the following corrective measures:

“a) Order the implementation of measures ensuring the association of the DPO with all data protection issues, in accordance with the requirements of Article 38 paragraph 1 GDPR. Although several ways can be envisaged to To achieve this result, one of the possibilities could be to analyze, with the DPO, all the relevant committees/working groups with regard to data protection and formalize the terms of its intervention (previous information with the agenda of meetings, invitation, frequency, permanent membership status, etc.).

b) Order the implementation of measures guaranteeing the autonomy of the DPO in accordance with the requirements of Article 38 paragraph 3 of the GDPR. Several measures can be envisaged to achieve this result, such as reporting the DPO to the highest management level in order to guarantee its autonomy as much as possible or the creation of a formalized and regular line of direct reporting, as well as an escalation mechanism management to bypass the hierarchical level(s) intermediary(ies).

c) Order the implementation of measures allowing the DPO to inform and advise the controller and the employees (who carry out the processing) on their data protection obligations pursuant to Article 39 paragraph 1 a) GDPR. Although several ways can be envisaged to achieve this As a result, one of the possibilities would be to set up formal reporting of the activities of the DPD to Management based on a defined frequency.

---

d) Order the deployment of the control mission, in accordance with article 39
paragraph 1 b) of the GDPR. The DPO should therefore document its controls relating to
application of internal data protection rules and procedures
(second line of defense). This documentation could take the form of a plan of
control. It should be noted that the execution of these checks is the responsibility of the DPO, who must
always control and supervise the work carried out in the event of delegation. »

78.

As for the corrective measures proposed by the head of investigation and with reference to point
69 of this decision, the Restricted Committee takes into account the steps taken by
controlled in order to comply with the provisions of Articles 38.1, 38.3, 39.1 a) and 39.1 b) of the
GDPR, in particular the measures described in his letters of December 12, 2019, October 14
2020 and June 26, 2021. More specifically, it takes note of the following facts:

- With regard to the violation of Article 38.1 of the GDPR, the Restricted Committee finds
that the audit has formalized the association of the DPO with questions relating to the protection
data by defining a specific frequency of participation of the DPO in the Committee
of management. 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 77 of the
this decision.

- With regard to the violation of Article 38.3 of the GDPR, the Restricted Committee finds
that the auditee made a change to the organization chart of the organization, published on 11
December 2019, so that the DPO is now attached directly to the
Department of General Services. The Restricted Committee therefore considers that there is no
place to pronounce the corrective measure proposed by the head of investigation and included under b)
of point 77 of this decision.

- With regard to the violation of Article 39.1 a) of the GDPR, the restricted training
understands that control has set up reporting of the activities of the DPO to the

Management based on a specific frequency (quarterly or biannual frequency). The

Restricted Committee therefore considers that there is no need to pronounce the measure

---

correction proposed by the head of investigation and repeated under c) of point 77 of this

decision.

- With regard to the violation of Article 39.1 b) of the GDPR, the restricted training is

of the opinion that it does not have the necessary documentation to determine with

sufficiency the exercise by the DPO of its mission of monitoring the compliance of the audit

GDPR. The Restricted Committee therefore considers that it is necessary to pronounce the measure

correction proposed by the head of investigation and repeated under d) of point 77 of this

decision.

In view of the foregoing developments, the National Commission sitting in formation

restricted, and deliberating unanimously decides:

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

- impose an administrative fine on Company A in the amount of

fifteen thousand four hundred euros (15,400 euros) with regard to the violation of articles 38.1,

38.3, 39.1 a) and 39.1 b) GDPR;

- issue against Company A an injunction to comply with the

Article 39.1 b) of the GDPR within four months of notification of the decision

restricted training, in particular:

ensure that the DPO can carry out his mission of monitoring the compliance of the

GDPR controller.

Thus decided in Belvaux on October 27, 2021.

The National Commission for Data Protection sitting in restricted formation

Commissioner

Tine A. Larsen Thierry Lallemang

President

Marc Lemmer

Commissioner

Indication of remedies

This administrative decision may be the subject of 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.
