Decision of the National Commission sitting in restricted formation on

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

Deliberation No. 10FR/2021 of March 26, 2021

The National Commission for Data Protection sitting in restricted formation,

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

Lemmer, commissioners;

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

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

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

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

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

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

adopted by decision no. 3AD/2020 dated January 22, 2020, in particular its article 10, point 2;

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

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

its article 9;

Considering the following:

I.

Facts and procedure

1.

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

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

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

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

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

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

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

Survey no. […] conducted with Company A.

1/15

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 […] Company A, established and having its registered office at L-[…] and entered in the register of

commerce and companies under number […] (hereinafter: “Company A” or the “controlled”) and

to appoint Mr. Christophe Buschmann as head of investigation. This deliberation specifies that

the investigation relates to Company A's compliance with Section 4 of Chapter 4 of the GDPR.

3.

The purpose of Company A is to carry out all insurance, co-insurance and

reinsurance, […]. At the end of the 2018 financial year, it employed […] people2 and it has

approximately […] customers per year3.

4.

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

preliminary draft to Company A to which the latter responded by letter dated October 3, 2018.

An on-site visit took place on January 30, 2019. Following these discussions, the head of investigation

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

5.

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

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

to know :

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

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

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

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

carry out its missions effectively;

2 Company A 2018 Annual Report.

3 Response provided by Company A in the preliminary questionnaire of September 17, 2018.

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 February 5, 2020 (hereinafter: the "statement of objections"), the head

of investigation has informed Company A of the breaches of the obligations provided for by the GDPR 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:

~

~

~

~

~

8.

the obligation to appoint the DPO on the basis of his professional qualities4;

the obligation to communicate the contact details of the DPO to the supervisory authority5;

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

personal data6;

the obligation to guarantee the autonomy of the DPO7;

the control mission of the DPD8.

By letter dated February 25, 2020, Company A sent the head of investigation its decision position on the shortcomings listed in the statement of objections. In what concerns the breach relating to the guarantee of the autonomy of the DPO, the person audited asserts in said letter that "the DPO is part of the team [...] reporting directly to the Director

4 Objective 4

5 Goal 3

6 Goal 8

7 Objective 7

8 Goal #10

General, the person to whom [the DPO] reports is the Chief Compliance Officer […]. The DPD does report directly to the General Manager, a recurring weekly meeting is moreover fixed and in case of emergency, an interview is fixed during the day. " Regarding breach relating to the control mission, Company A asserts, in its letter of 25 February 2020, that “[a] control plan had been drawn up for 2019 (see appendix 2), it was presented on 15/01/2019 and validated by […]) […]”. The controller also transmitted additional documents by email of August 26, 2020, namely two examples relating to the operation and passages through the […] and the […].

9.

On September 4, 2020, the head of investigation sent Company A a letter complementary to the statement of objections by which he informs the auditee that following his position paper of February 25, 2020 and documents provided by email dated August 26, 2020,

the grievances relating to the DPO's autonomy and control tasks should be lifted. Was attached to the letter of 4 September 2020 an amending statement of objections (hereinafter: the “amending statement of objections”) incorporating the corrective measures that the head of inquiry proposes to the National Commission sitting in restricted formation (hereafter: the “restricted formation”) to adopt.

10.

By letter dated September 15, 2020, Company A sent the head of investigation its comments on the amending statement of objections.

11.

During the examination of the investigation file, the restricted committee did not noted other elements that would constitute a breach relating to the autonomy or to the control mission of the DPO.

12.

The matter was on the agenda of the Restricted Committee meeting on 13 November 2020. In accordance with Article 10, point 2, letter b) of the internal rules of the National Commission, the head of investigation and the controller presented oral observations on the case and answered the questions posed by the Restricted Committee. Company A had speak last.

II.

Place

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

1. On the principles

13.

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 […]”.

14.

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”.

15.

In addition, the Article 29 Data Protection Working Party has adopted on 13 December 2016 guidelines concerning DPOs which have been taken over and re-approved by the European Data Protection Board on May 25, 20189.

These guidelines specify that the level of expertise of the DPO “must be proportionate to the sensitivity, complexity and volume of data processed by an organization”10 and that “it It is necessary for DPOs to have expertise in the field of legislation and national and European data protection practices, as well as a in-depth knowledge of the GDPR”11.

16.

The DPO Guidelines continue that “[k]nowledge of the 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

17.

It appears from the audit report that as part of this audit campaign, the head of investigation expects the DPO to have at least three years of professional experience in data protection.

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

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

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

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

18.

According to point 20 of the amending statement of objections, it was noted during the investigation that the DPO has less than three years of experience in data protection data and that prior to taking office in […] 2018, he held the position of […]. Point 21 of the amending statement of objections lists the events and training sessions related to data protection which the DPO attended after taking of function.

19.

Nevertheless, the head of investigation considers that these trainings are not sufficient to establish the existence of sufficient expertise adapted to the needs of the controller in data protection matters at the time of the investigation such that there is a breach to the obligation provided for in Article 37(5) of the GDPR.

20.

In its position papers of February 25 and September 15, 2020, Company A argues

that the DPO continue to follow training courses and participate in events and groups of

work in connection with data protection so that the DPO will have reached three years

of experience in […] 2021.

21.

It is thus apparent from the amending statement of objections and the positions of the

verified that prior to taking office in […] 2018, the DPD had no

professional experience in data protection.

22.

The Restricted Committee takes note that in 2018 and 2019, the DPO attended a number of

number of training sessions and events relating to data protection. She rallies

however, to the finding of the head of investigation that these trainings are not sufficient to establish,

at the time of the investigation, the existence of sufficient expertise adapted to the needs of the

data protection control.

23.

In view of the foregoing, the Restricted Committee concludes that Article 37(5) of the GDPR

was not complied with by Company A.

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

control

1. On the principles

24.

Article 37(7) of the GDPR provides for the obligation for the organization to communicate the

contact details of the DPO to the supervisory authority. Indeed, it follows from Article 39(1) e) of the GDPR

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

that the latter has the contact details of the DPO.

25.

The DPO Guidelines explain in this respect that this requirement

aims to ensure that “supervisory authorities can easily and directly take

contact with the DPO without having to go to another department of the body”13.

26.

It should also be noted that the CNPD published on its website as of May 18

2018 a form allowing organizations to send it the contact details of their

DPD.

2. In this case

It follows from the audit report that the head of investigation expects the organization to have

27.

communicated on May 25, 2018 the contact details of its DPO to the CNPD.

28.

According to point 24 of the amending statement of objections, Company A

communicated to the CNPD the contact details of the DPO who was in office at the time of the investigation

by email of […] 2018. The DPO previously in place was not declared

in application of the GDPR.

29.

In its position paper of February 25, 2020, the controller maintains that the contact details

of the first DPO were communicated on […] 2017 and that when he left […], he was

replaced by the current DPO.

30.

The Restricted Committee notes that the GDPR has been applicable since May 25, 2018 from

so that the obligation to communicate the contact details of the DPO to the supervisory authority exists

since that date.

31. Even if the data protection officer as provided for by the repealed law of 2

August 2002 on the protection of individuals with regard to the processing of personal data

personal character can be called a precursor to DPD insofar as there are

similarities between the two functions, the fact remains that there are differences,

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

---

particularly at the level of designation and old and new legislation. Thus, the

data protection officers designated under the repealed law of 2 August 2002

did not automatically take on the function of DPO and the bodies which had appointed

voluntarily such an officer under the old law still had to comply with the

articles 37 to 39 of the GDPR, and in particular communicate the contact details of the DPO to the CNPD.

32.

In any case, it appears from the audit report that the former protection officer

of data was not designated as DPO but that an internal […] performed this function

between May 25, 2018, date of entry into application of the GDPR, and […] 2018, date of

depending on the DPO currently in office. However, the contact details of the DPO who was in office

between May 25, 2018 and […] 2018 were not communicated to the CNPD. Contact details

of the DPO currently in office were communicated on […] 2018.

33.

In view of the foregoing, the Restricted Committee concludes that Article 37(7) of the GDPR

was not complied with by Company A.

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

the protection of personal data

1. On the principles

According to Article 38(1) of the GDPR, the organization must ensure that the DPO is associated,

34.

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

personal data.

35.

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

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

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

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

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

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

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

data processing activities within the organisation”14.

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

36.

The DPO Guidelines provide examples on how

to ensure this association of the DPO, such as:

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

intermediate ;

- to recommend the presence of the DPO when decisions having implications in

data protection matters are taken;

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

 consult the DPO immediately when a data breach or other

incident occurs.

37.

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

develop data protection guidelines or programs

indicating the cases in which the DPO must be consulted.

2. In this case

38.

It appears from the audit report that as part of this audit campaign, the head

of investigation expects the DPO to participate in a formalized manner and on the basis of a frequency

defined to the Management Committee, the project coordination committees, the

new products, safety committees or any other committee deemed useful in the context of

Data protection.

39.

According to points 28 and 29 of the amending statement of objections, the DPO participates

mainly by ad hoc invitation to the various control committees, such as the

[…], […] or […], without regular and systematic participation being provided for. the

DPD is informed by the controller […] of the discussions taking place at […]. Accounts

rendered […] are sent to the DPO who does not participate in these meetings.

40.

In its position papers of February 25 and September 15, 2020, Company A argues

that the DPO participates personally in a systematic way in the […] and that he participates

also at […] on an ad hoc basis for data protection matters. For

all projects or significant changes in a process, the Project Manager must

systematically complete a questionnaire […] which is submitted to the DPO […] for evaluation

impacts on data protection and triggering of an impact analysis if

---

necessary. The controller further maintains that the DPO is informed of any new project thanks to

to his participation in […].

41.

The Restricted Committee notes that in point 30 of the amending statement of objections,

the head of investigation comes to the conclusion that "[w]hile it is not disputed that the operation

of the controller allows the DPO to be reasonably informed about the issues

protection of personal data, the absence of a mechanism allowing

the regular and systematic personal involvement of the DPO is not such as to guarantee a

sufficient level of association adapted to the needs of the data controller. »

42. Although it is true that Article 38(1) of the GDPR does not require the organization to

puts specific measures in place to ensure that the DPO is involved in all matters

relating to the protection of personal data, it is also true that the lines

guidelines on DPOs, which provide recommendations and best practices,

guide data controllers in compliance with their

governance. However, the Restricted Committee did not identify any elements in the investigation file

leading to the conclusion that the DPO was not involved, in an appropriate and timely manner

useful for all questions relating to the protection of personal data.

43.

In view of the foregoing, the Restricted Committee concludes that the breach of Article

38(1) GDPR does not exist.

III.

On the corrective measures and the fine

44.

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 of the GDPR.

45.

According to Article 58(2) of the GDPR, "[e]ach supervisory authority shall have the authority to adopt all of the following corrective measures:

(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. »

46.

In the amending statement of objections, the head of investigation proposes to the

restricted training to take the following corrective action: “Put in place the measures

allowing the DPO (or a dedicated "Data Protection" team) to acquire expertise

sufficient and adapted to the needs of the data controller in terms of data protection.

data, in accordance with the provisions of Article 37, paragraph (5) of the GDPR and the lines

Article 29 Data Protection Working Party DPO Guidelines

which specify that the level of expertise of the DPO must be proportionate to the sensitivity,

complexity and volume of data processed by the organization. The continuation of the effort to

formation of the DPO is one possibility to achieve this result. »

47.

The head of investigation also proposes to “[t]et in place the measures allowing

to involve the DPO in all matters relating to data protection, in accordance with

the requirements of Article 38 paragraph 1 of the GDPR. Although several ways can

considered to achieve this result, one of the possibilities could be to strengthen

the personal and systematic involvement of the DPO in the various relevant committees. " Being

given that the Restricted Committee considers that the breach alleged by the Head of Investigation

on the obligation to involve the DPO in all matters relating to the protection of

data is not constituted, there is no need to examine the related corrective measure.

48.

Finally, given the facts observed at the start of the investigation and the

particular circumstances of the case, the head of investigation suggests to the restricted formation of

not retain an administrative fine in addition to the corrective measures.

A. The call to order

49.

Under Article 58(2) b) of the GDPR, the CNPD may call to order a person responsible

of the processing or a processor when the processing operations have led to a violation

provisions of the GDPR.

50.

In view of the fact that the control violated Article 37(5) and (7) of the GDPR, the training

Restricted considers that it is justified to issue a call to order against the Company

HAS.

B. Compliance of processing operations

51.

Under Article 58(2) d) of the GDPR, the CNPD may order the person responsible for the

processing or the processor to bring the processing operations into compliance with the

GDPR, if applicable, in a specific manner and within a specific time frame.

52.

As for the violation of Article 37(5) of the GDPR providing for the obligation to designate the

DPD on the basis of his professional qualities, it is apparent from point 34 of the communication

of the amending grievances that the auditee has “proactively implemented a program of

training for the DPO both on the protection of personal data, on the

cybersecurity or the security of information systems only on the […] and operation

of the controller". Consequently, the Restricted Committee considers that there is no

no need to pronounce a compliance measure in this respect, especially since the

DPD will soon be able to demonstrate three years of professional experience in

Data protection.

53.

Regarding the violation of Article 37(7) of the GDPR providing for the obligation to communicate

the contact details of the DPO to the supervisory authority, the Restricted Committee finds that the Company

A communicated to the CNPD the contact details of the DPO currently in office by email of the

[…] 2018. Consequently, the Restricted Committee considers that there is no need to pronounce

a compliance measure in this regard.

C. The administrative fine

54.

Under Article 58(2) i) of the GDPR, the CNPD may impose a fine
administrative procedure pursuant to Article 83, in addition to or instead of the measures referred to
to this paragraph, depending on the specific characteristics of each case. Section 48(1) of the
Law of August 1, 2018 on the organization of the National Commission for the Protection of
data and the general data protection regime specifies that the CNPD may
impose administrative fines as provided for in Article 83 of the GDPR, except
against the State or the municipalities.

55.

According to Article 83(2) of the GDPR, "[t]o decide whether to impose a fine
administrative and to decide on the amount of the administrative fine, he is duly required
account, in each specific case, of the following elements:

(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 pursuant to

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 adverse effects thereof;

(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

breach;

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

ordered against the controller or processor concerned for

the same object, compliance with these measures;

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

certification mechanisms approved under section 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. »

56.

It follows from point 34 of the amending statement of objections that the head of investigation

took into account “the facts at the time of the opening of the investigation and the following elements:

~

The fact that the DPO is a cornerstone of the principle of accountability and that he

either at the heart of the legal framework established by the GDPR;

~

The fact that it is undisputed that the operation of the controller

allows the DPO to be reasonably informed;

The fact that the data controller has proactively implemented a program

training for the DPO both on the protection of personal data, on

cybersecurity or the security of information systems only on the […] and of the

functioning of the controller".

57.

Thus, the head of investigation suggests to the restricted formation not to withhold a fine

administrative in addition to corrective measures.

58.

The restricted formation agrees with the developments of the head of investigation and considers by

therefore that there is no need to impose an administrative fine on the Company

HAS.

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

restricted formation and deliberating unanimously decides:

to rule against Company A, established and having its registered office at L-[…] and registered

in the trade and companies register under number […], a reminder to have

violated Article 37 (5) and (7) of the GDPR.

Thus decided in Belvaux on March 26, 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.
