Decision of the National Commission sitting in restricted formation

on the outcome of investigation No. […] conducted with Company A

Deliberation No. 19FR/2021 of May 31, 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 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:

_____

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

Survey No. […] conducted with Company 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 (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 and having its registered office at L-[…] and registered in the trade and
companies under number […] (hereinafter: “Company A” or the “controlled”) and to designate Mr.
Christophe Buschmann as head of investigation. Said deliberation specifies that the investigation concerns
on Company A's compliance with Section 4 of Chapter 4 of the GDPR.

3.

The purpose of the control is to carry out all insurance, co-insurance and
reinsurance […] in the Grand Duchy of Luxembourg. At the beginning of 2019, Company A
employed about […] employees at the company's headquarters (not taking into account the people
in the various branches) and had approximately […] customers […]2.
By letter dated September 17, 2018, the head of investigation sent a questionnaire

4.

preliminary draft to Company A, to which the latter responded by letter dated October 8, 2018.
on-site visit took place on January 18, 2019. Following these exchanges, the head of investigation established the
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 Report of the Visit of January 18, 2019.

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

Survey No. […] conducted with Company A

5.

It appears from the audit report that in order to verify the compliance of the organization with the section

4 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 23, 2019 (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 a

failure to ensure that the tasks and tasks of the DPO do not lead to

conflict of interest 3.

3 Goal 5

8.

By letter dated November 21, 2019, Company A sent the head of investigation its decision

position on the failure listed in the statement of objections. The control says

in the said letter that "various measures are already implemented within Company A

and more generally of the group […] to avoid such a conflict of interest" and that the roles of Chief

Compliance Officer and DPD have been occupied by different people since […] 2019.

On August 10, 2020, the head of investigation sent Company A an additional letter

9.

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

grievances") by which he informs the control of the corrective measure that the head of investigation proposes

to the National Commission sitting in restricted formation (hereinafter: the "restricted formation")

to adopt.

By letter dated September 17, 2020, the controller sent the head of the investigation his

10.

comments on the supplementary statement of objections.

The case was on the agenda of the restricted committee meeting of January 26, 2021.

11.

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

head of investigation and the control presented oral observations on the case and responded to the

questions asked by the Restricted Committee. The controller spoke last.

II.

Place

1. On the principles

12.

According to Article 38.6 of the GDPR, “[the DPO] may perform other missions and tasks. the

responsible for processing or the processor ensures that these missions and tasks do not entail

no conflict of interest”.

13.

The guidelines for DPOs4 specify that the DPO cannot practice within

of the organization a function which leads it to determine the purposes and means of the processing of

personal data. In general, among the functions likely to

give rise to a conflict of interest within the organization may include the functions

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

senior management (for example: general manager, operational manager,

financier, chief medical officer, marketing department manager, resource manager

human resources or IT manager), but also other roles at a lower level

of the organizational structure if these functions or roles imply the determination of the purposes

and means of treatment. In addition, there may also be a conflict of interest, for example,

if an external DPO is called upon to represent the controller or processor

before the courts in cases relating to matters relating to the protection of

data.

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

the vacancy notice for the function of DPO or the service contract is sufficiently precise

and detailed to avoid any conflict of interest. In this context, it is also appropriate to

keep in mind that conflicts of interest can take different forms depending on whether the

DPD is recruited internally or externally.

2. In this case

14.

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

achieved by the audited within the framework of this audit campaign, the head of investigation expects that

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

functions do not entail a conflict of interest, in particular through the exercise of functions which

would lead the DPO to determine the purposes and means of the processing of personal data

personal. The head of investigation also expects the person to be checked to have carried out an analysis

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

15.

According to the Statement of Objections, it appears from the investigation that the DPO is also Chief Compliance Officer of the audited body and that this other function involves a risk of conflict of interest, particularly in the context of the department's AML/KYC processing Compliance. Consequently, the DPO would be involved in setting up data processing personal data in the context of his duties as Chief Compliance Officer.

16.

In its position papers of November 21, 2019 and September 17, 2020, Company A points out the existence, in January 2019, of various measures aimed at avoiding such conflict of interest.

17.

Company A explains on the one hand that its structural organization consists of three defense lines:

- A first line of defence, […];
- A second line of defense […];
- A third line of defense […].

18.

According to Company A, this concept of the three lines of defense "makes it possible to best prevent conflicts of interest in any field combined by organizing a segregation of the different functions. Thus, the function of DPO within Company A, […], excludes processing the data relating to AML/KYC processing and the purposes and means of the processing are decided

only by the teams […]. The DPO within Company A may need to

decide on the compliance of the processing implemented by the teams […], […]".

19.

Company A also adds in its position paper of November 21, 2019 that "the

Chief Compliance Officer only checks that the decisions taken […] comply with the

group requirements […] and applicable laws and standards and acts only as advice; he

ensures the efficiency and effectiveness of controls over AML/KYC operational activities

as such, […]".

On the other hand, Company A has an internal conflict management policy and

20.

external parties, providing that in the event of a potential conflict of interest that would impact the function of DPO,

the latter shall inform the […] and the […] in order to take the necessary measures.

21.

In addition, it appears from the positions taken by Company A on November 21, 2019 and November 17

September 2020 that the control appointed in […] 2019 a new DPO so that the

functions of DPO and Chief Compliance Officer are no longer combined in the head of a

single person. The new DPO also performs the duties of […] of Company A.

The Restricted Committee takes note of the existence of these measures in order to limit the risks

22.

conflict of interest within the audited body. She agrees, however, with the observation of the chief

of investigation according to which the implementation of these various measures would not be sufficient to establish,

at the time of the survey, the absence of any risk of conflict of interest in the context of the duties of the

DPD. Indeed, it is not sufficiently established that the Chief Compliance Officer, combining this function with that of DPD at the time of the investigation, does not participate in the determination of purposes and means of the processing of personal data implemented in the framework of AML/KYC operational activities.

23.

In view of the foregoing, the Restricted Committee concludes that Article 38(6) of the GDPR has no not been complied with by Company A.

III.

On the corrective measures and the fine

A. Principles

24.

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 CNPD has the powers provided for in Article 58.2 of the GDPR:

(a) notify a controller or processor of the fact that the operations of envisaged processing are likely to violate the provisions of this Regulation;

b) call to order a data controller or a processor when the operations of processing have resulted in a breach of the provisions of this Regulation;

(c) order the controller or processor to comply with requests submitted by the data subject with a view to exercising their rights under this these regulations;

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

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

specific manner and within a specified time;

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

personal data breach;

impose a temporary or permanent restriction, including a ban on processing;

f)

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

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

recipients to whom the personal data has been disclosed in

application of Article 17, paragraph 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 certification body to

not to issue a certification if the requirements applicable to the certification are not

or more satisfied;

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

i)

place 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. »

25.

In accordance with article 48 of the law of August 1, 2018, the CNPD may impose fines

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

municipalities.

26.

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 in deciding whether to impose

an administrative fine 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, taking into account

the technical and organizational measures that they have implemented under the

sections 25 and 35;

e) any relevant breach previously committed by the controller or the

subcontracting ;

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

f)

and mitigate any negative effects;

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

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

the extent to which the controller or processor notified the breach;

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

i)

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 violation. »

27.

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.

28.

Nevertheless, the steps taken by the controller to comply with

the GDPR in the course of the investigation procedure or to remedy the breaches noted by the

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

restricted in the context of any corrective measures to be taken.

B. In the instant case

1. Regarding the imposition of an administrative fine

It follows from the statement of objections and the statement of objections

29.

additional that the head of investigation does not propose an administrative fine against the

control.

30.

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

Therefore, there is no need to impose an administrative fine against Company A.

2. As to the call to order

31.

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.

32.

Given that the control violated Article 38(6) of the GDPR, the restricted training

considers that it is justified to issue a call to order against Company A.

3. Regarding the taking of corrective measures

33.

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

Restricted Panel to take the following corrective action: “Order the implementation of

measures ensuring that the various missions and tasks, current or past, of the person

carrying out the DPO function do not give rise to a conflict of interest in accordance with the requirements of

Article 38 paragraph 6 of the GDPR. Although several ways can be implemented

to achieve this result, one of the possibilities would be to involve a third party, benefiting

the necessary skills, for the review of the treatments for which there is a conflict interest (in this case AML/KYC processing). Another possibility would be to occupy the post of DPO by a person different from the Compliance Officer and not having another risk of conflict.

34.

With reference to point 21 of this decision, the Restricted Committee takes into account the steps taken by the controller following the statement of objections sent to the controller by the head of investigation, in order to comply with the provisions of Article 38.6 of the GDPR, as detailed in these letters of November 21, 2019 and September 17, 2020. More specifically, the Restricted Committee takes note of the fact that the Control appointed, in […] 2019, a new DPO so that the functions of DPO and Chief Compliance Officer are no longer combined under a single person and that the new DPO also performs the functions of […] of Company A.

35.

However, the Restricted Committee considers that the audit did not demonstrate that the appointment of a new DPO, with the separation of the functions of Chief Compliance Officer,

was sufficient in itself to eliminate any risk of conflict of interest in the exercise of the DPO assignments. Consequently, the Restricted Committee considers that the controlled party has not has sufficiently demonstrated its compliance with Article 38.6 of the GDPR and that it is necessary to issue a compliance measure in this regard.

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

- to pronounce against […] Company A, a call to order with regard to the violation

Article 38.6 of the GDPR;

- to pronounce against […] Company A, an injunction to comply

with Article 38.6 of the GDPR, within four months of notification of the

decision of the Restricted Committee, the supporting documents for compliance must be

addressed to the restricted training at the latest within this period, in particular:

eliminate any risk of conflict of interest in the performance of his duties by the DPO.

Thus decided in Belvaux on May 31, 2021.

For 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.
