Decision of the National Commission sitting in restricted formation on

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

Deliberation No. 38FR/2021 of October 15, 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:

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

survey no.[…] conducted with public establishment 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 public establishment A, established in L[…], and registered in the trade and companies register under the number J[…] (hereinafter: the "controlled") and to designate Mr. Christophe Buschmann as chief investigator. Said deliberation specifies that the investigation relates to the compliance of the controlled with section 4 of chapter 4 of the GDPR.

3.

The control is a public establishment […] under the supervision of the Ministry […]. […] Control has as mission […]

4.

By letter dated September 17, 2018, the head of investigation sent a questionnaire preliminary to the audit, to which the latter responded by letter dated October 5, 2018. first on-site visit took place on 24 January 2019, a second on-site visit took place on 27 May 2019 and additional information was received on July 23, 2019. Following these exchanges, the head of investigation drew up 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.

5.

It appears from the audit report that in order to verify compliance of the audit with 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 February 14, 2020 (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 this letter of February 14, 2020.

7.

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

breaches of:

□

□

the obligation to publish the contact details of the DPO2;

the obligation to appoint the DPO on the basis of his professional qualities3;

2 Objective 2

3 Objective 4

8.

□

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

of a personal nature4;

the obligation to provide the necessary resources to the DPO5;

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

□

□

conflict of interest6;

□

the control mission of the DPD7.

On August 10, 2020, the head of the 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.

The controller responded to the additional letter to the statement of objections by a letter dated September 14, 2020 in which he presents his observations for each failure recognized by the head of the investigation.

10.

In addition, the controller, on October 28, 2020, requested access to the investigation file concerning him. Access to the investigation file was sent to him by the National Commission on 9 November 2020.

The president of the restricted formation informed the control by letter of April 12, 2021

11.

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 25, 2021 that he would participate in said session.

During the restricted training session of June 16, 2021, the head of investigation and the

12.

controlled presented their oral observations on the case and answered the questions posed by restricted formation. The controller spoke last.

4 Objective 8

5 Objective 6

6 Goal 5

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

survey no.[…] conducted with public establishment A

The controller provided additional information by email of June 17, 2021, following

13.

to a request in this sense from the restricted formation.

II.

Place

A. On the breach of the obligation to publish the contact details of the DPO

1. On the principles

14.

Article 37.7 of the GDPR provides for the obligation for the controlled body to publish the

contact details of the DPO. Indeed, it follows from Article 38.4 of the GDPR that the persons concerned

must be able to contact the DPO regarding any questions relating to the

processing of their personal data and the exercise of the rights conferred on them by the

GDPR.

15.

The DPO Guidelines explain in this regard that this requirement is aimed at

ensure that “affected persons (both inside and outside the organization)

can easily and directly contact the DPO without having to go to another

service of the body”. The guidelines also state that "the contact details of the

DPD must contain information allowing data subjects to reach it

easily (a postal address, a specific telephone number and/or a

specific email)”.8

In addition, Article 12.1 of the GDPR provides that the controller must take

16.

appropriate measures to provide any information referred to in Articles 13 and 14 of the GDPR in

regarding the processing to the data subject in a concise, transparent,

understandable and easily accessible, in clear and simple terms. Among the information

which must be transmitted to the person concerned is the information relating to the contact details

of the DPO, in accordance with Articles 13.1.b) and 14.1.b) of the GDPR.

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

---

2. In this case

17.

It appears from the audit report that, for the head of investigation to consider objective 2 as

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

that the audited body publish the contact details of its DPO internally within the body

and externally with the public representing the data subjects of the processing. the

DPD must be easily and directly contactable via an appropriate communication channel

To those concerned. Active internal communication is expected, in particular via

emails, newsletters or even dedicated spaces on the intranet. Externally it is at least

whereas the contact details of the DPO are easily accessible on the website of

the organism.

18.

It appears from the statement of objections that, during the first visit by the officers of the

CNPD in charge of the investigation on January 24, 2019, the contact details of the DPD were difficult to

find on the website of the controlled insofar as, on the one hand, the website did not contain

no section dedicated to data protection and, on the other hand, the information notice relating

Data Protection was only available in English, with no translation in any of the

official languages of Luxembourg.

The controller made changes during the investigation to remedy this.

19.

problem. In fact, it initially created a data protection section on

its website and, in a second step, added links to download

French and German versions of the information notice in PDF format.

The Head of Investigation therefore concluded in the Statement of Objections that, during

20.

investigation, the contact details of the DPO had become more easily accessible for

persons concerned.

However, as explained on page 2 of the Statement of Objections, “[t]he facts considered

21.

account in the context of this [statement of objections] are those noted at the beginning of

investigation. The modifications made subsequently, even if they ultimately allow

to establish the compliance of the data controller, do not make it possible to cancel a breach

found. »

22.

In this context, the Restricted Committee notes that the GDPR has been applicable since 25

May 2018 so that the obligation to publish the contact details of the DPO, as well as the principle of

transparency as set out in Article 12.1 of the GDPR, have existed since that date. Publish the contact details of the DPO on a website without taking the necessary measures to ensure that the people concerned are able to find the information and understand it render meaningless the obligation of Article 37.7 of the GDPR.

In view of the foregoing, the Restricted Committee concludes that Article 37.7 of the GDPR has no

23.

not respected by the controller.

B. On the breach of the obligation to appoint the DPO on the basis of his qualities professional

1. On the principles

24.

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 […]”.

25.

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”.

26.

Furthermore, the guidelines of the Article 29 Working Party on DPOs specify that the level of expertise of the DPO “must be proportionate to the sensitivity, complexity and the volume of data processed by an organization”9 and that “it is necessary that DPOs have expertise in the field of national laws and practices and

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

data protection regulations, as well as an in-depth knowledge
GDPR”10.

The DPO Guidelines go on to state that “[a]knowledge of the

27.

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
that information systems and the needs of the data controller in terms of
data protection and security”11.

2. In this case

28.

It appears from the audit report that, as part of this audit campaign, for the
head of investigation considers objective 4 as achieved by the control, the head of investigation expects
that the DPO has at least three years of professional experience in data protection
Datas.

29.

According to the Statement of Objections, page 3, on the date the audit was launched, a DPO
was on duty and “[t]he had all the skills required in terms of
legal (lawyer registered with the Luxembourg Bar) and data protection (certificate
CIPP/E)”.

A new internal DPO was however appointed during the investigation, in April 2019.

30.

According to the statement of objections, page 3, this new internal DPO "is also responsible
[…] and he has knowledge of the domain and the structure. Nevertheless, it should be

find that he has no initial training in legal matters, data protection and

data processing, nor does it justify a previous practice in the matter".

In its position paper of September 14, 2020, the auditee wished to highlight the

31.

difficulties he had to face in recruiting a DPO with the right profile, namely a

experienced person with knowledge of the functioning of the […] sector. the

board of directors qualifies the first external recruitment as an "attempt

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

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

---

failed" and chose to appoint as DPO an experienced internal employee who is able to

to understand the challenges of the […] sector and the regulatory complexity that characterizes it. the

audited considers that this knowledge of the profession is an important and priority criterion for

regard to its specific sector.

The controller adds that the new internal DPO has followed several training courses in terms of

data protection between 2017 and 2019, regular weekly coaching with

the assistance of a specialist data protection law firm was in place

since April 2019 and that the DPO has participated monthly since December 2018 in the sessions

of the informal public sector working group […].

In addition, the DPO has the possibility of relying on a daily basis, for the performance of his tasks,

on the contribution of the teams […] and, on the IT department, on the legal department, on

the risk management expert and any other internal resource deemed useful. Since September

2017, the control set up "GDRP points of contacts", consisting of the designation

of a few people belonging to the various control trades to be the relay

of the DPD12.

32.

The Restricted Committee notes that, according to the Head of Investigation, the training relating

to data protection which the internal DPO has attended since his appointment, as well as

the fact that he has access to a certain number of internal and external supports in the execution of his

missions, cannot be sufficient to establish, at the time of the appointment of the new internal DPO,

the existence of sufficient expertise adapted to the needs of the auditee in terms of protection

data13.

33.

However, as noted on page 2 of the statement of objections, "[t]he facts

taken into account in this case are those observed at the start of the investigation".

However, the Restricted Committee notes that at the start of the investigation, an external DPO was in

34.

function and, as noted by the head of investigation and repeated in point 29 of this

12 Report of the visit of January 24, 2019, page 3

13 Statement of Objections, page 3.

decision, he possessed all the skills required in legal matters and in

data protection.

In view of the foregoing, the Restricted Committee concludes that there is no reason to accept a

35.

breach of Article 37.5 of the GDPR.

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

36.

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.

37.

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 organization”.

The DPO Guidelines provide examples on how

38.

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.

39.

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

40.

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.

41.

According to the Statement of Objections, page 4, the external DPO who was in office at the start
of the audit had an essentially “reactive” role. “[His] involvement was therefore
relatively limited. He intervened mainly at the explicit request of the head of the
treatment and not spontaneously”. The audit report, page 9, specifies that the involvement
limitation of the external DPO was characterized more particularly by a “weak participation in the
recurring meetings, only by invitation when the need has been estimated”.

In its position paper of September 14, 2020, page 6, the auditee considers that the

42.

description by the Head of Investigation of the essentially reactive role of the external DPO in charge of

start of the investigation is inaccurate and amounts to minimizing the involvement of the external DPO, as in

certifies the statement of hours worked on several projects […].

The new internal DPO, for his part, takes part more easily in the various meetings of

43.

projects. The feedback of information is facilitated by the proximity and the various relays in place

in structure. Furthermore, according to the audit report, page 9, the internal DPO is a guest

standing committee of the auditing executive committee (frequency every two weeks) and one point

systematic “GDPR” is on the agenda of every board meeting which takes place every

three months.

However, according to the audit report, page 9, a precise circuit concerning the opinions to be given by

the DPO is not yet clearly defined, due to the recent designation of the internal DPO.

In its position paper of September 14, 2020, the auditee informs the CNPD about the

44.

implementation of an internal process ([…]) to formalize and document the association of the DPO

data protection issues. This internal process is implemented

systematically for each new activity […] of the controlled and aims to allow:

- prior documentation and systematic reporting of information to the DPO before

the implementation of the controlled processing, and this at the latest at the time of the

in place of contracts,

-

upstream identification of sensitive data protection points,

the upstream review of the information notices and consent forms distributed

[…],

 Raising the awareness of operational teams and discussions with them, in

a privacy by design approach, and

planning or performing data protection impact assessments.

45.

The audit also specifies that the association of the DPO with issues of data protection

data is also carried out on the initiative of the teams or the DPO himself within the framework of the review

documentation, the co-signing of contracts relating to data protection, the design of

projects […] of the control, the assistance of the internal teams in the realization of the analyzes

of impact and the participation of the DPO in the executive committee as a permanent guest.

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

46.

internal formalization and documentation of the involvement of the new internal DPO in matters

relating to data protection. Whether these measures should facilitate the association of the DPO

internal to all questions relating to data protection, it is nevertheless necessary to

note that these were decided during the investigation.

47.

Indeed, as explained on page 2 of the statement of objections, “[t]he facts taken into

account in the context of this [statement of objections] are those noted at the beginning of

investigation. The modifications made subsequently, even if they ultimately allow

to establish the compliance of the data controller, do not make it possible to cancel a breach

found. »

The Restricted Committee is of the opinion that the auditee has not sufficiently demonstrated

48.

the association of the external DPO, in office at the start of the investigation, in an appropriate manner and

in good time to all questions relating to data protection.

49.

Consequently, the restricted committee agrees with the observation of the head of investigation according to which,

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

External DPO was appropriately involved in all matters relating to protection

personal data.

50.

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

not been respected.

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

1. On the principles

According to Article 39.1 b) of the GDPR, the DPO has, among other things, the mission of “monitoring compliance

51.

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”. Recital (97) specifies

that the DPO should help the organization verify internal compliance with the GDPR.

52.

It follows from the DPO Guidelines15 that the DPO may, in the context of
its 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 5, “it appears from the investigation that the body does not
does not have formalized controls specific to data protection. In a logic
day-to-day management of data protection, and given the volume of data
processed and the sensitivity of some of this data (see preliminary remarks), it is
whereas the control missions of the DPO are better formalized, for example with
establishment of a control plan.

In its position paper of September 14, 2020, the controlled party indicates that the control of the

55.

compliance of the data controller with the GDPR is ensured thanks to the implementation of

following means:

the legal review of the processing register of the controlled by a law firm

-

specialized in data protection, from January to October 2019,

- an internal audit outsourced to an audit firm on organizational aspects,

- an external audit carried out by an audit firm, in order to assess the compliance of the control

[…].

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

56.

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

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

controller and processor16”.

57.

In addition, the Restricted Committee notes that it is rightly specified on page 2 of the

statement of objections (under “preliminary remarks”) that “the requirements of the GDPR do not

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 controllers at the

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

concerned”.

58.

In this context, the Restricted Committee is of the opinion that it is possible for an organization to

use external service providers to verify its compliance with the GDPR. However, this call

to external service providers must be formalized, and this must not result in

completely remove this mission from the DPO function. Indeed, the DPO of the organization must complete

its task of monitoring compliance with the GDPR by participating in the formalization of a control plan

and by being associated with the exercise of said control by external service providers, in particular by

accompanying the work carried out, in order to then be able to fill in knowledge of

causes its mission of advice and information in accordance with article 39.1 a) of the GDPR.

In this case, the person inspected did not demonstrate that, at the start of the investigation, an inspection plan

59.

compliance with the GDPR would have been formalized nor that the external DPO then in office was associated with the

control carried out by external service providers. Consequently, the Restricted Committee is of the opinion

that the auditee does not sufficiently demonstrate that the external DPO in office at the start of

the survey fulfilled this control mission expected by Article 39.1 b) of the GDPR.

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

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

60.

not respected by the controller.

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

1. On the principles

61.

Article 38.2 of the GDPR requires the organization to help its DPO “to carry out the tasks

referred to in Article 39 by providing the resources necessary to carry out these missions, as well as

as access to personal data and processing operations, and allowing it

to maintain their specialist knowledge.

62.

It follows from the DPO Guidelines that the following aspects should

in particular be taken into consideration17:

- “sufficient time for DPOs to perform their tasks. This aspect is

particularly important when an internal DPO is appointed on a part-time basis or when

the external DPO is responsible for data protection in addition to other tasks.

Otherwise, conflicting priorities could lead to the DPO's tasks being

neglected. It is essential that the DPO can devote sufficient time to his

assignments. It is good practice to set a percentage of time devoted to the function

of DPD when this function is not full-time. It is also good

practical to determine the time required to perform the function and the level of

appropriate priority for the tasks of the DPO, and that the DPO (or the body) establishes a

workplan ;

- necessary access to other departments, such as human resources, service

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

essential support, input and information from these other services”.

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

63.

The DPO Guidelines state that “[b]e generally, more
the processing operations are complex or sensitive, the more resources granted to the DPO
should be important. The data protection function must be effective and equipped with
adequate resources with regard to the data processing carried out”.

2. In this case

64.

It emerges from the audit report that, given the size of the organizations selected within the framework
of this audit campaign, so that the head of investigation considers objective 6 as fulfilled by the
controlled, he expects the controlled to have at least one FTE (full-time equivalent) for
the data protection team. The chief investigator also expects
the DPO has the possibility to rely on other services, such as the legal service,
IT, security, etc.

65.

According to the audit report, the external DPO in charge at the start of the investigation had a role
essentially “reactive”. The hour readings of this one fluctuate between 20 hours and 108
hours per month, i.e. between 0.125 FTE and 0.7 FTE.

The monthly distribution of these hours worked by the external DPO is detailed in the

66.

report of the on-site visit of May 27, 2019, page 2, as follows: 8 p.m.
September 2018, 53 hours in October 2018, 57.2 hours in November 2018, 50.4 hours in
December 2018, 122.2 hours in January 2019, 103.9 hours in February 2019 and 108.6 hours in

March 2019. The Restricted Committee notes that this therefore makes an average of 73.6 hours performed per month over this 7-month period, i.e. an average monthly FTE of 0.46.

In view of these elements, the Restricted Committee understands that the external DPO has

67.

began to work hours as part of its missions only from September

2018. In addition, most of his hours were worked between January and March 2019.

However, the Restricted Committee recalls that the GDPR came into force on May 25, 2018.

68.

It is therefore from May 2018 that the audited body had the obligation to comply with the GDPR by designating a DPO exercising his function effectively and efficiently.

69.

The audit report indicates that the new internal DPO estimated his time for

work on data protection issues at more than 70% of the entire

his tasks. It is also specified that legal support by an external firm has been obtained

at the rate of one day per week, the sole legal competence of the controller cannot provide only limited support to the internal DPO. The controller also benefited from the assistance of a audit firm in the conduct of the "GDPR" roadmap of the control.

70.

In the statement of objections, page 4, the head of investigation specifies that "given the existence of complex or sensitive processing operations (see preliminary remarks), a high level of resources is expected". However, the head of the investigation notes that "the new DPD [internal], who also holds the position of manager […] for [the auditee], assessed

the time devoted to his duties as DPO to more than 70%" and that "the controller

has not been able to demonstrate the accomplishment of the control missions. This

finding is likely to highlight a mismatch between the resources and means

made available to the DPO and the needs of the controller".

In its position paper of September 14, 2020, the controller indicates that the new DPD

71.

internal, also responsible […] at the time of his appointment, is now Head of

Compliance […], assisted by four other people for the management of responsibilities related to

compliance and risk management. According to the controller, the presence of these four other

people allows the Head of Compliance […] to focus on the DPO functions.

In addition, to enable the Head of Compliance […] to take on the role of internal DPO,

72.

the auditee has made available a budget enabling it to use external legal support

and proper technique.

Finally, as noted in point 55 of this decision, the audited indicates in its decision

73.

of position of September 14, 2020, that the mission of monitoring compliance with the GDPR by the controlled

is carried out with the help of external service providers such as audit and law firms

specialized. The auditee is of the opinion that the audit mission provided for in Article 39.1 b) of the GDPR

is ensured and therefore that the resources and means provided for the purposes of such control are appropriate

to the needs of the control.

74.

The Restricted Committee recalls that, as indicated in the communication

objections, page 2, and already noted in point 21 of this decision, “[t]he facts taken into account

in the context of this [investigation] are those found at the start of the investigation. The

modifications made subsequently, even if they ultimately make it possible to establish the

compliance of the data controller, do not make it possible to cancel a breach

found. »

In addition, the Restricted Committee agrees with the finding of the head of investigation that

75.

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

preliminary), a high level of resources is expected” and that “the head of the

processing has not been able to demonstrate the completion of the control tasks.

This finding is likely to highlight a mismatch between resources and

means made available to the DPO and the needs of the controller”.

Consequently, the Restricted Committee is of the opinion that the auditee was unable to demonstrate

76.

with sufficiency that the audit provided the external DPO in office at the start of the investigation with the

resources necessary to enable it to carry out its missions.

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

77.

not respected by the controller.

F. On the failure to ensure that the other missions and tasks of the DPO

do not involve a conflict of interest

1. On the principles

78.

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".

79.

The DPO Guidelines18 specify that "the DPO may not exercise on the
within the organization a function that leads it to determine the purposes and means of the processing
of personal data". According to the guidelines, "as a general rule, among
positions that may give rise to a conflict of interest within the organization may include
senior management functions (for example: general manager, operational manager,
financial director, chief medical officer, head of the marketing department, head of
human resources or head of IT), but also other roles at a
lower level of the organizational structure if these functions or roles involve the
determination of the purposes and means of processing. Additionally, there may also be
conflicts of interest, for example, if an external DPO is called upon to represent the head of the
processing or the processor before the courts in matters relating to matters
related to data protection.

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

80.

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

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

where the DPO exercises other functions within the audited body, these functions do not entail

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

no 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. The head of investigation

also expects that the auditee has carried out an analysis as to the existence of a possible

conflict of interest at DPO level.

81.

According to the Statement of Objections, page 5, "[t]he DPO who was in office at the beginning of

the audit was external and lawyer. There is a principle for managing conflicts of interest. »

The new DPO subsequently appointed internally also exercised the function of

82.

responsible […]. The statement of objections notes that "possible conflicts of interest are

likely to exist in view of the tasks performed for the two positions. Based on

comments of the DPO dated 12/08/2019, there exists within [the auditee] a policy of

management of potential conflicts of interest. However, the analysis of conflicts of interest between two functions exercised by the same person within the same [public institution] is not planned. There is therefore no analysis of potential conflicts of interest between the DPO function and that of responsible […]. Based on the DPO's comments dated 12/08/2019, the [checked] will make sure to clarify the different job descriptions concerning the management of aspects related to data protection in order to distinguish more clearly the authorities, responsibilities and assignments".

83.

In its position paper of September 14, 2020, the controller indicates that the internal DPO is now Head of Compliance […] of the organization. It also specifies that the records of Head of Compliance and Risk Manager functions have been modified to include more clearly the responsibilities and missions related to data protection.

84.

The auditee's conflict of interest policy was also updated in July 2020, in order to introduce an obligation to analyze the risks of conflict of interest in the presence of a accumulation of functions and have them arbitrated by the Board of Directors of the audited.

85.

The controlled also argues that the externalization of several aspects of the control of the compliance implemented to date allows control to eliminate the risk of conflicts interest in the control of management-related processes […]. Indeed, several aspects

checking the compliance of the controlled processing (in particular those implemented in framework of the exercise of the Compliance function) have been entrusted to external service providers,

as raised in point 55 of this Decision.

86.

By email dated June 17, 2021, the control sent to the restricted training the

conflict of interest policy as updated in July 2020.

87.

The Restricted Committee recalls that, as indicated on page 2 of the

statement of objections and already noted in point 33 of this decision, “[t]he facts taken into

account in the context of this [investigation] are those found at the beginning of the investigation”.

The Restricted Committee notes that, at the start of the investigation, the DPO in office was a DPO

88.

who worked as a lawyer at the Luxembourg Bar. The principles

ethics to which the lawyers of the Luxembourg Bar are subject include the

principle according to which a lawyer cannot represent or assist parties with interests

opposed, nor represent or assist a client in the event of a conflict with the personal interests of

the lawyer himself.19 This ethical principle is applicable to any lawyer registered with the Bar of

Luxembourg under the amended law of 10 August 1991 on the legal profession and the Regulation

Interior of the Luxembourg Bar Association as adopted by the Bar Council

dated January 10, 2013, without there being any obligation on the part of customers to verify the

due observance by the lawyer of this principle.

Consequently, the CNPD is of the opinion that it was not up to the data controller to

89.

check with its external DPO to ensure there is no conflict

potential interests with other customers and/or subcontractors of the controlled, but that on the contrary,

this obligation fell to the external DPO pursuant to the amended law of 10 August 1991 on

the legal profession and ethical rules.

90.

In view of the foregoing, the Restricted Committee concludes that there is no reason to accept a breach of Article 38.6 of the GDPR.

19 Website of the Luxembourg Bar, The profession of lawyer, Ethics: https://www.barreau.lu/le-metier-d-lawyer/ethics

---

III.

On the corrective measures and the fine

A. Principles

91.

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. »

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

92.

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;

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

survey no.[…] conducted with public establishment A

24/33

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;

i)

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

93.

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.

94.

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

95.

In his supplementary letter to the statement of objections of 10 August 2020, the head of investigation proposes to the restricted formation to pronounce against the controlled a fine administrative relating to the amount of 27,100 euros.

96.

In order to decide whether to impose an administrative fine and to decide, if applicable, of the amount of this fine, the Restricted Committee analyzes the criteria laid down by GDPR Article 83.2:

- As to the nature and gravity of the breach [Article 83.2 a) of the GDPR], with regard to breaches of Articles 37.7, 38.1, 38.2 and 39.1 b) of the GDPR, restricted training 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 persons concerned have the possibility of easily finding the contact details of the DPO to exercise their rights to data protection, as well as in the event that the DPO has the resources necessary for the exercise of its missions, is associated with all issues relating to data protection and performs its duties effectively, including the mission 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 person inspected modified its website during the investigation in order to to make the contact details of the DPO more easily accessible for people concerned. In particular, a French and German translation have been added to the website of the auditee in August 2019. The breach of article 37.7 of the GDPR therefore lasted in time, at least between May 25, 2018 and August 2019.

(2) the controller informed the CNPD, in its position paper of September 14, 2020, of the implementation of an internal process for formalizing and documenting

the involvement of the new internal DPO in matters relating to the protection of data ([…]) from October 17, 2019. These measures were nevertheless decided under investigation. The breach of Article 38.1 of the GDPR therefore lasted in the time, at least between May 25, 2018 to October 19, 2019.

(3) it has not been demonstrated by the auditee that the external DPO in office at the time of the opening of the investigation had the necessary resources for the exercise of its missions and that, according to the audit report, the new internal DPO estimates his time work on data protection issues at around 70% compared to his other duties. The breach of Article 38.2 of the GDPR therefore lasted in the time, from May 25, 2018, it being specified that the restricted training could not find that the breach has ended.

(4) it has not been demonstrated by the control that both the external DPD in function at the start of the investigation that the new internal DPO fulfilled their mission of monitoring the compliance of the organization with the GDPR as part of their daily functions, the controlled having chosen to call on external service providers, without demonstrated the involvement of the external and internal DPOs in the organization of the control. The breach of Article 39.1 b) of the GDPR therefore lasted over time, at from May 25, 2018, it being specified that the Restricted Committee was unable to ascertain that the breach has ended.

- 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.

- as to the categories of personal data concerned by the breach

[article 83.2 g) of the GDPR], the restricted training takes into account the fact that the controlled processes

special categories of personal data […].

97.

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.

98.

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 93 of this decision).

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

99.

is justified with regard to the criteria set out in article 83.2 of the GDPR for breaches of articles

37.7, 38.1, 38.2 and 39.1 b) GDPR.

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

Article 83.3 of the GDPR provides that in the event of multiple infringements, as is the case here,

the total amount of the fine cannot exceed the amount fixed for the most serious violation. In

the extent to which a breach of Articles 37.7, 38.1, 38.2 and 39.1 b) of the GDPR is attributed to the

checked, the maximum amount of the fine that can be withheld is 10 million euros or

2% of worldwide annual revenue, whichever is higher.

101. With regard to the relevant criteria of Article 83.2 of the GDPR mentioned above, the training Restricted considers that the imposition of a fine of 18,000 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

102. In his supplementary letter to the statement of objections of 10 August 2020, the head of investigation proposes to the Restricted Committee to take the following corrective measures:

“a) Order the implementation of measures allowing the DPO (or a “Data” team Dedicated protection) to acquire sufficient expertise adapted to the needs of the responsible for data protection in accordance with the provisions of Article 37, paragraph (5) of the GDPR and the guidelines on the DPD of the “article 29” working party on data protection 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. Although several ways can be envisaged to achieve this result, one of the possibilities could be to provide a formal internal or external support in terms of IT skills to your DPO, and enroll them in accelerated/intensive training in data protection. data. The measures mentioned by the controller during the audit, such as that access to external expertise for any need for legal assistance should be maintained, or even reinforced, in view of the sensitivity of the data processed;

b) Order the implementation of measures ensuring formalized and documented association of the DPO on all questions relating to data protection in accordance with the requirements of Article 38 paragraph 1 of the GDPR and the principle of “accountability”. Good

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

possibilities could be to analyze, together with the DPO, all the committees/working groups

relevant with regard to data protection and to formalize the terms of its

intervention (previous information on the agenda of meetings, invitation, frequency, status

permanent member, etc.);

c) Order the implementation of measures guaranteeing the necessary resources for the

DPD in accordance with the requirements of Article 38 paragraph 2 of the GDPR. Although

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

possibilities could be to relieve the DPO of all or part of its other

missions/functions or to provide support, internally or externally, with regard to the exercise

of its DPO missions;

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

current or past, of the person exercising the function of DPO do not lead to

conflicts of interest in accordance with the requirements of Article 38 paragraph 6 of the GDPR.

Although several ways could be implemented, one of the possibilities would be

the involvement of a third party with the necessary skills; for the

review of processing for which there is a risk of conflict of interest (review of the

---

risk management, review of processes concerning the various treatments present,

review of job descriptions and/or job descriptions, etc.);

e) Order the formal and documented deployment of the DPO monitoring mission

in accordance with Article 39 paragraph 1 b) of the GDPR and the principle of “accountability”.

The DPO must carry out his supervisory tasks, in accordance with Article 39 paragraph 1

b) GDPR. Although several ways can be envisaged to achieve this

result, the DPO should always document his checks on the application of the rules and

internal data protection procedures (second line of defence).

This documentation could take the form of a control plan followed by reports. »

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

102 of this decision, the Restricted Committee takes into account the steps taken

by the controlled in order to comply with the provisions of Articles 37.5, 38.1, 38.2, 38.6 and 39.1 b)

of the GDPR, in particular the measures described in its letter of September 14, 2020. More

in particular, it takes note of the following facts:

- With regard to compliance by the controller with article 37.5 of the GDPR, the training

restricted notes that, following the appointment of the new internal DPO, he followed

several training courses in data protection so that he has

sufficient expertise to perform their duties. However, as noted

in point 35 of this decision, the Restricted Committee considers that there is no need

to retain a breach of Article 37.5 of the GDPR with regard to the situation of the controlled

at the start of the investigation. Consequently, the Restricted Committee does not pronounce the measure

correction as proposed by the head of investigation and repeated under a) of point 102 of the

this decision.

- With regard to the violation of Article 38.1 of the GDPR, the controller indicates in its

letter of September 14, 2020 that an internal process of formalization and documentation

the involvement of the new internal DPO in matters relating to the protection of

data […]) was set up by the controller. The Restricted Committee considers as soon as

when there is no need to pronounce the corrective measure proposed by the head of investigation and repeated under (b) of point 102 of this decision.

- Regarding the violation of Article 38.2 of the GDPR, the internal DPO currently in function estimated its working time on data protection issues at about 70% compared to his other tasks. Given the fact that the audited processes a substantial amount of data whose degree of sensitivity may be relatively high, the Restricted Committee considers that the DPO should have more resources for the performance of its duties. The Restricted Committee therefore considers that there is reason to pronouncing the corrective measure proposed by the head of investigation and repeated under c) of point 102 of this decision.

- With regard to the organization's compliance with article 38.6 of the GDPR, the training restricted considers that the auditee did not demonstrate that, despite the accumulation of functions internal DPD and Head of Compliance […], sufficient internal measures would have been taken in order to avoid that the DPO will not be called upon to decide on the processing whose aims and means he would have helped to determine. However, like this was noted in point 90 of this decision, the Restricted Committee considers that there is no there is no reason to hold a breach of Article 38.6 of the GDPR with regard to the situation of the checked at the beginning of the investigation. Therefore, the restricted formation does not pronounce the corrective measure as proposed by the head of investigation and repeated under d) of point 102 of this decision.

- With regard to the violation of Article 39.1 b) of the GDPR, the restricted training is of the opinion that the audit has not demonstrated that the DPO currently in office fulfills his mission of control of the respect of the RGPD by the controlled, the latter having chosen to make use of external service providers to ensure this control, without any evidence of the involvement of the new internal DPO in the organization of this control work. The Restricted Committee therefore considers that it is appropriate to pronounce the corrective measure

proposed by the head of investigation and reproduced under e) of point 102 of this decision.

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

restricted formation and deliberating unanimously decides:

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

- to pronounce against the public institution A an administrative fine of one

amount of eighteen thousand euros (18,000 euros) with regard to the violation of articles 37.7,

38.1, 38.2 and 39.1 b) GDPR;

- to pronounce against the public establishment A an injunction to put itself in

compliance with Article 38.2 of the GDPR within six months of the notification of

the decision of the Restricted Committee, in particular:

ensure that the DPO has the necessary resources for the exercise of his

assignments;

- to pronounce against the public establishment A an injunction to put itself in

compliance with Article 39.1 b) of the GDPR, within six months of notification

the decision of the Restricted Committee, in particular:

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

Thus decided in Belvaux, on October 15, 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.
