Decision of the National Commission sitting in restricted formation

on the outcome of survey no.[…] conducted with

Company A

Deliberation No. 18FR/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 relating

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

personnel 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 its article 41;

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

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 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- […], entered in the register of commerce and companies under the number […] (hereinafter: the "controlled") and to designate Mr. Christophe Buschmann as head of investigation. This deliberation specifies that the investigation concerns the compliance of the control with section 4 of chapter 4 of the GDPR.

3.

The purpose of the audit is in particular […]2. The control has about […] employees spread over […] sites as well as […]3.

4.

By letter dated September 17, 2018, the head of investigation sent a questionnaire preliminary to the control to which the latter replied by letter of October 5, 2018. A visit on site took place on January 21, 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 Coordinated articles of association filed on […].

3 Presentation of the audit of January 21, 2019

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;

5) Ensure that the missions and tasks of the DPO do not lead to a conflict of interest;

6) Ensure that the DPO has sufficient resources to carry out effectively

of its missions;

7) Ensure that the DPO is able to carry out his duties with a sufficient degree

autonomy within their organization;

8) Ensure that the organization has put in place measures for the DPO to be associated with

all questions relating to data protection;

9) Ensure that the DPO fulfills his mission of providing information and advice to the

controller and employees;

10) Ensure that the DPO exercises adequate control over data processing within

of his body;

11) Ensure that the DPO assists the controller in carrying out the

impact analyzes in the event of new data processing.

6.

By letter dated October 31, 2019 (hereinafter: the “statement of objections”), the head

of investigation informed the control of the breaches of the obligations provided for by the RGPD that it

found during his investigation. The audit report was attached to that letter.

7.

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

breaches of:

~

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

personal data4;

~

~

the obligation to provide the necessary resources to the DPO5;

the information and advice mission of the DPO6.

4 Objective 8

5 Objective 6

6 Goal #10

8.

By letter dated November 22, 2019, the inspector sent the head of the investigation his decision position on the shortcomings listed in the statement of objections.

9.

On August 24, 2020, the head of investigation sent an additional letter to the controller to the statement of objections (hereinafter: the "additional letter to the statement of grievances") by which he informs the control of the corrective measures and the administrative fine that it proposes to the National Commission sitting in restricted formation (hereafter: the " restricted formation") to adopt.

10.

By letter dated September 30, 2020, the controller sent the head of the investigation his comments on the additional letter to the statement of objections.

11.

The case was on the agenda of the Restricted Committee meeting on January 26 2021. In accordance with Article 10.2. b) the internal rules of the Commission national, the head of the investigation and the controller presented their oral observations in support of their written submissions. More specifically, Master […], agent of the audited, gave reading of a note setting out the observations of the auditee (hereinafter: the "pleadings note"). The head of investigation and the controller then answered the questions posed by the training restraint. The controller spoke last.

12.

By email of January 27, 2021, the authorized representative of the control sent to the training restricted a copy of the pleadings note, an excerpt from a presentation dated October 8 2018 presenting the "Data Protection" organization chart with indication of the "[GDPR Committee]" of the controlled party as well as an extract from the register of commerce and companies of […] Company B

manager […] in Luxembourg.

II.

Place

A. Regarding the requirements for precision in the statement of objections and the letter supplementary to the Statement of Objections

13.

In his pleadings, the auditee's representative invokes, as a preliminary point, that the statement of objections and the supplementary letter to the statement of objections lack precision:

"[...] the Courriers de Grief breach the applicable legal obligations in terms of administrative, in particular in that they do not contain any precise reference to a standard legal which would have been violated and that they do not contain any precise indication of the facts details that would constitute a violation of a legal standard by Company A. By this lack of precision, the general principles of applicable law have been violated and my principal was deprived of the opportunity to provide informed and detailed explanations likely to enlighten the Restricted Training. »

14.

The Restricted Committee notes that the head of investigation expressly mentions, both in the statement of objections and in the supplementary letter to the statement of the grievances, the provisions of the GDPR which the control would have breached, namely articles 38.1, 38.2 and 39.1. has). Furthermore, the factual findings made during the investigation and on which the alleged breaches are based are set out in the Statement of Objections. Of

surplus, the audit report containing all the findings and work carried out by the head

inquiry as part of the audit mission was attached to the Statement of Objections. In

In addition, the Restricted Committee notes that the auditing agent refers to the

“legal obligations applicable in administrative matters” as well as the “general principles

of applicable rights” without specifying which rule of law would have been violated in

the species.

15.

For all intents and purposes, it should be noted that the auditee was able to take

position in relation to the breaches of which it is accused, as demonstrated by its

position of 22 November 2019 and 30 September 2020 as well as the oral observations and the

note of pleadings presented at the restricted committee session of January 26, 2021.

16.

It is therefore wrong that the agent of the controlled maintains that the communication of the

objections and the supplementary letter to the statement of objections lack the precision of

so that his principal would have been "deprived of the possibility of providing enlightened explanations

and detailed information likely to inform the Restricted Training”.

B. As to the objections listed in the statement of objections

a) On the breach of the obligation to involve the DPO in all matters relating to the

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,

17.

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

personal data.

18.

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 organization”.

The DPO Guidelines provide examples on how

19.

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

with regard to data protection are taken;

always give due consideration to the opinion of the DPO;

immediately consult the DPO when a data breach or other

incident occurs.

20.

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

21.

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

as achieved by the auditee as part of this audit campaign, the head of investigation

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

expects the DPO to participate in a formalized way and on the basis of a defined frequency

to the Management Committee, to the project coordination committees, to the committees of new

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

Datas.

22.

According to the Statement of Objections, page 3, “the DPO participates in many

meetings at Group level and […] regularly organizes meetings with its points of

local contacts. But these elements are not sufficient to demonstrate the direct, formal and

of the involvement of the DPD in Luxembourg". It also results from the communication of

grievances that "the Group DPO receives a monthly report from the local contact point following

to […] as well as a monthly report […] relating to data protection issues

(number of requests to exercise rights or complaints, any impact analyzes

etc.). […] the DPO is systematically informed and consulted by the local contact point in

case of a security incident likely to involve personal data and

to create a risk for the persons concerned. The head of the investigation, however, believes that "these elements cannot compensate for the lack of direct involvement of the DPD Groupe within Company A, which could create the risk that the DPO is not sufficiently involved at the operational level in Luxembourg. Finally, the head of investigation argues that he "did not have knowledge of elements allowing this risk to be addressed, such as for example the formal establishment of visits based on a defined frequency of the DPO Group (or a member of its Data Protection team) in Luxembourg. These visits would allow the DPO in particular to be able to discuss directly with management superior of the Company Has issues related to data protection and power directly assess operational issues. »

23.

In its position paper of November 22, 2019, the auditee states that the DPD Groupe is involved in an appropriate and timely manner in all matters relating to the protection of personal data. The auditee states that "[a]ll questions relating to the protection of personal data initiated in the Grand Duchy of Luxembourg are received and analyzed initially by our point of contact dedicated to the data protection in Luxembourg" (hereinafter: the "local contact point") and that this the latter works in close collaboration with the DPD Group […]. According to the controlled, the point of contact is responsible for managing the compliance of personal data processing staff implemented by the control, this under the supervision of the Group DPD to whom the point of contact reports his actions. In addition, the auditee mentions in his statement

of 22 November 2019 the establishment of a committee dedicated to data protection in Luxembourg

(hereinafter: the “[GDPR Committee]”) which defines the strategy on these subjects and the action plans associates. The audited sets out the composition and functioning of the [GDPR Committee] for maintain that the Group DPO is involved in managing compliance with the provisions GDPR in Luxembourg.

In his note of pleadings, the agent of the audited puts forward article 37.2 of the

24.

GDPR, which allows a group of companies to appoint a single DPO provided that the latter be easily reachable from each place of establishment, as well as the guidelines regarding DPOs to support that the operation of the controlled is GDPR compliant and affirms that “[i]t was found no materiality of the alleged facts, no unavailability of the DPO of Company A, whether vis-à-vis the supervisory authority or even of the persons concerned and a possible and uncharacterized risk cannot allow to factually establish a violation. »

25.

The Restricted Committee notes that the auditee is a subsidiary of the group […] and that the latter had decided to appoint a single DPO for the various entities of the group (hereafter after: the “Group DPO”). At the central level, the group has set up an office of the data protection (“[…]”) composed of the Group DPO as well as […] lawyers specialized in data protection and […] project manager. At local level, the sole control lawyer has been appointed as the local point of contact for the Group DPD.

26.

As a preliminary point, the Restricted Committee finds that the breach alleged by the Chief investigation relates to Article 38.1 of the GDPR so that the explanations of the agent of the checked regarding Article 37.2 of the GDPR are not relevant in this case. In effect, even if the GDPR authorizes a group of companies to appoint a single DPO, the fact remains however, this DPO must be associated, in an appropriate and timely manner, with all

questions relating to the protection of personal data, in accordance with

GDPR Article 38.1. It is thus permissible for an organization to designate a single DPO at the level

of the group whose entities are established in several Member States of the European Union

and to provide, at local level, "contact points" which assist the DPO in particular in

issues relating to local particularities such as national legislation. In such

case, it is however all the more important to clearly define, among other things, the

methods of collaboration between the DPO and the “local contact points” as well as the

distribution of tasks and responsibilities.

In this case, the Restricted Committee notes that all questions relating to the protection of

personal data that arose at the level of the controlled were received and

initially analyzed by the local contact point who contacted the Group DPO

when he deemed it necessary. The Restricted Committee further notes that the DPD Group did not

not part of the [GDPR Committee] and was only informed of the subjects discussed there through the

[GDPR Committee] verbal meetings and through the questions raised by the point of

local contact at these meetings.

27.

It appears from the investigation file that the Group DPO was not associated

only indirectly to questions relating to the protection of personal data

which arose at the level of the controlled, this through the intermediary of the local point of contact which,

in fact, acted as interlocutor in terms of data protection within

of the organism. However, the local point of contact was the only legal expert in the audit and did not

part of the Group DPD team proper, namely the data protection office

data (" […] ").

28.

Moreover, the Restricted Committee considers that the fact of transmitting the minutes of the [GDPR Committee] to the Group DPD does not establish its proper association and in timely insofar as the Group DPO is simply informed of the measures that the [GDPR Committee] proposes to the various decision-making bodies of the control to implement. The DPO is therefore not informed and above all not consulted “from the earliest stage possible” of all questions relating to data protection.

29.

In addition, the auditee indicates in its position paper of September 30, 2020 that the local point of contact has been appointed as DPO for Company A, with effect from 1 October 2020. The Restricted Committee finds that the CNPD received the amending declaration by email of September 30, 2020. However, the controller must ensure that the newly appointed is effectively involved in all matters relating to data protection of a personal nature. Having named the local contact point as DPO is not enough not to sufficiently demonstrate such an association of the latter to all questions relating to the protection of personal data.

30.

In view of the foregoing, the Restricted Committee agrees with the finding of the head of investigation that non-compliance with Article 38.1 of the GDPR was established at the time of the investigation.

---

b) On the failure to provide the necessary resources to the DPO

1. On the principles

31.

Article 38.2 of the GDPR requires the organization to help its DPO “to carry out the tasks
referred to in Article 39 by providing the resources necessary to carry out these tasks, as well as
that access to personal data and processing operations, and
to maintain their specialist knowledge. »

32.

It follows from the DPO Guidelines that the following aspects should
in particular to be taken into consideration8:

~ “sufficient time for DPOs to perform their tasks. This aspect is
particularly important when an internal DPO is appointed on a part-time or
when the external DPO is in charge of data protection in addition to other
tasks. Otherwise, conflicting priorities could lead to the tasks of the
DPD are neglected. It is essential that the DPO can devote enough
time on his assignments. It is good practice to set a percentage of time
devoted to the function of DPO when this function is not occupied full time.
It is also good practice to determine the time required to complete the
the appropriate function and level of priority for the DPO's tasks, and that the DPO (or
organization) draw up a work plan;

~ necessary access to other services, such as human resources, the service
legal, IT, security, etc., so that DPOs can
receive essential support, input and information from these other
services ".

33.

The DPO Guidelines state that “[b]eally,

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

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

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

2. In this case

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

34.

It appears from the audit report that, given the size of the organizations selected, for

that the head of investigation considers objective 6 as achieved by the control within the framework of

this audit campaign, the head of investigation expects the audit to employ at least

one FTE (full-time equivalent) for the data protection team. Leader

of investigation also expects the DPO to have the possibility of relying on other

services, such as legal, IT, security, etc.

It appears from the Statement of Objections, page 3, that the Group DPO has at the level

center of a team made up of […] lawyers specializing in the protection of

data as well as […] project manager. At local level, however, the Group DPO does not have

than a local point of contact who was also the only lawyer of the audited so that the

head of investigation notes "the risk that the DPO does not have enough resources at the level

local in Luxembourg, the resources being concentrated at the level of the group, but not seeming

not sufficiently deployed at the local level" as well as "the risk that in the event of a strong peak

of activity concerning legal matters to be handled within Company A, the point of contact

local may not have the means to effectively carry out its missions relating to

data protection, which would create the risk that the DPO would not be able to exercise

effectively carry out its tasks as DPO for Luxembourg".

35.

In its position paper of November 22, 2019, the auditee states that the DPD Groupe

has the support of a local legal team made up of the local point of contact

and a “second resource” and notes that “the job description of the Local Point of Contact

and the second resource in the local legal team on a permanent contract

must be detailed in terms of the number of hours and the description of the tasks”.

36.

In his note of pleadings, the agent of the audited also argues that

the requirement to formalize the distribution of working time does not exist in the regulations

applicable and that the DPO Guidelines contain at most one

recommendation as a “good practice” to “determine the time required to

the performance of the function and the appropriate level of priority for the tasks of the DPO, and that the

DPD (or the body) establishes a work plan”. Finally, the agent of the controlled

maintains that “[i]t has, here again, no materiality of the alleged facts, nor provided

no explanation of the criteria examined to conclude that there was a lack of resources, nor

no analysis of existing resources. A possible and uncharacterized risk cannot

make it possible to establish factually that Company A would lack the resources to deal with

its data protection obligations. »

37.

The Restricted Committee notes that the controller has opted to designate the Group DPO

which has, at the central level, a team made up of […] lawyers specializing in

data protection as well as […] project manager. Entity level

Luxembourg that was the subject of the investigation, a local point of contact was appointed,

person of the only lawyer of the control who also exercised other missions. The

Restricted Committee considers that such an organization requires the organization to determine and

documents the time required for the local point of contact to perform its related tasks

to data protection in order to be able to allocate the necessary resources. This

requirement results in particular from the guidelines concerning the DPOs as well as from the articles

5.2. and 24 of the GDPR which set out the principle of accountability. However, it emerges

of the file that the auditee has not carried out any formalization or documentation

making it possible to demonstrate that the audit has provided the DPD function with the resources

necessary for the exercise of its missions at the time of the investigation.

38.

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

not respected by the controller.

c) On the breach relating to the mission of information and advice of the DPO

1. On the principles

39.

Under Section 39.1. a) of the GDPR, one of the tasks of the DPO is to “inform and

advise the controller or processor as well as the employees who carry out

processing on their obligations under this Regulation and other

provisions of Union law or the law of the Member States relating to the protection of

data ".

2. In this case

40.

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

as achieved by the audited within the framework of this audit campaign, it expects that “

the organization has formal reporting of the activities of the DPO to the Management Committee on based on a defined frequency. Regarding employee information, it is expected that the organization has set up an adequate staff training system on data protection".

41.

According to the statement of objections, page 4, it appears from the investigation that there is no direct feedback of information from the Group DPD to the local control department. Leader of investigation notes that "there are several levels of reporting ([…])", but considers that "these elements are not sufficient to compensate for the lack of direct reporting from the DPO to the data controller in Luxembourg".

42.

In its position paper of November 22, 2019, the auditee refers to these explanations relating to the first complaint, namely the breach of the obligation to involve the DPO in all issues relating to the protection of personal data. Furthermore, the control maintains that the Group DPO "informs and advises the data controller as well as the employees and has notably implemented:

o Online Training […], available online from May 2018

o An awareness campaign with […] on the protection of personal data personnel on […] 2018, as well as on […] 2019[…]

o An Awareness Campaign with […] including the 10 golden rules on the protection of personal data dated […] 2019"

The controller also asserts that the Group DPD "has the opportunity to discuss subjects

strategic and/or more operational with the senior management […] of Company A".

43.

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

44.

The Restricted Committee considers that the mission of information and advice of the DPO to with regard to the controller is closely linked to the obligation, provided for in Article 38.1 of the GDPR, to involve the DPO in an appropriate and timely manner in all questions relating to the protection of personal data. However, the restricted formation has noted that the Group DPO was not involved in an appropriate and timely manner with the data protection issues arising at the level of the Luxembourg entity having

is under investigation. Indeed, the Group DPD was only indirectly associated, that is by through the local point of contact. Moreover, he was simply informed of the measures that the [GDPR Committee] proposes to the various supervisory decision-making bodies to implement work.

45.

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

III.

On corrective measures and fines

A. Principles

46.

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

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;

9 Points 26 to 30 of this decision

---

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. »

47.

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

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

or municipalities.

48.

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

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

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

instead of imposing an administrative fine and to decide the amount of this fine:

“(a) the nature, gravity and duration of the breach, 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, 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

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

breach ;

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

ordered against the controller or processor concerned for

the same purpose, compliance with these measures;

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

certification mechanisms approved under Article 42; and

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

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

or indirectly, by reason of the breach".

49.

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.

50.

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

with the GDPR in the course of the investigation procedure or to remedy the breaches

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

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

B. In the instant case

1. Regarding the imposition of an administrative fine

51.

In the additional letter to the statement of objections of 24 August 2020, the

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

administrative fine in the amount of 18,000 euros.

52.

In his note of pleadings, the agent of the control argues that a fine

administrative “must meet the principles of adequacy and proportionality of Article 83

of the GDPR while in particular, no specific grievance has been formulated, no prejudice has been

noted and Company A has collaborated as far as possible with the CNPD during

the entire control period. »

53.

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

concerns breaches of Articles 38.1, 38.2 and 39.1 a) of the GDPR, training

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

efficient and effective, namely to facilitate compliance with the GDPR by the organization, that in

the case where the DPO is associated from the earliest possible stage with all

data protection issues, has the resources and time

necessary to carry out its tasks relating to data protection and exercises

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

controller. A breach of Articles 38.1, 38.2 and 39.1 a) of the GDPR

amounts to reducing the interest, even to emptying of its substance, the obligation for an organization

to appoint a DPO.

- As for the duration criterion (Article 83.2.a) of the GDPR), the Restricted Committee notes that

the auditee indicated, in its position paper of September 30, 2020, that the point of

local contact has been appointed as DPO with effect from 1 October 2020 and that this

latter now devotes 50% of his working time to protection issues

data, with the assistance of […] other lawyers who also devote

each 50% of their working time. Furthermore, the composition and functioning of the

[GDPR Committee] have been modified so that the DPO can inform and advise

the controller. Breaches of Articles 38.1, 38.2 and 39.1 a) have

therefore lasted over time, at least between May 25, 2018 and October 1, 2020.

The Restricted Committee recalls here that two years separated the entry into force of the

GDPR of its entry into force to allow data controllers to

comply with their obligations.

- As to the number of data subjects affected by the breach and the level of

damage they have suffered (Article 83.2 a) of the GDPR), the Restricted Committee notes that

the control has approximately […] employees spread over […] sites as well as […]. the

number of people affected by the breach is therefore potentially high.

- As to the degree of cooperation established with the supervisory authority (Article 83.2 f) of the

GDPR), the restricted training takes into account the assertion of the head of investigation according to

which the auditee has shown constructive participation throughout

investigation.

54.

The Restricted Committee notes that the other criteria of Article 83.2 of the GDPR do not

are neither relevant nor likely to influence its decision on the imposition of a fine

administrative and its amount.

55.

The Restricted Committee notes that while several measures have been put in place by the

checked in order to remedy in whole or in part certain shortcomings, these have only been

adopted only following the launch of the investigation by CNPD officials on 17

September 2018 (see also point 49 of this decision).

56.

Therefore, the Restricted Committee considers that the imposition of a fine

administrative is justified with regard to the criteria laid down by article 83.2 of the GDPR for

breach of Articles 38.1, 38.2 and 39.1 a) of the GDPR.

57.

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

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

case, the total amount of the fine may not exceed the amount set for the most serious violation.

severe. Insofar as a violation of Articles 38.1, 38.2 and 39.1 a) of the GDPR is

accused of the controlled, the maximum amount of the fine that can be withheld is 10

million euros or 2% of worldwide annual revenue, whichever is greater

retained.

58.

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

Restricted Committee considers that the pronouncement of a fine of 18,000 euros appears at the

effective, proportionate and dissuasive, in accordance with the requirements of Article 83.1 of the GDPR.

2. Regarding the taking of corrective measures

59.

In his supplementary letter to the statement of objections, the head of investigation

proposes to the Restricted Committee to take the following corrective measures:

“(a) Order the establishment of measures ensuring a formal association and

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

would consist in analyzing, together with the DPO, all the committees/working groups relevant to the

with regard to data protection and to formalize the terms of its intervention
(previous meeting agenda information, invitation, frequency, status of
permanent member etc).
b) Order the provision of the necessary resources to the DPO in accordance with
the requirements of Article 38 paragraph 2 of the GDPR. Although several ways
could be considered to achieve this result, one of the possibilities would be
to relieve the DPO and/or the local members of his team of all or part of his
other missions/functions or to provide formal support, internally or externally,
regarding the performance of its DPO duties.
c) Order the implementation of measures allowing the DPO to inform and advise
formally inform the data controller of his obligations in terms of protection
data, in accordance with Article 39 paragraph 1 a) of the GDPR. Although
several ways can be envisaged to achieve this result, one of the
possibilities would be to put in place formal reporting of the activities of the DPO to the
Direction based on a defined frequency. »
60.
As for the corrective measures proposed by the head of investigation and with reference to the
point 50 of this decision, the Restricted Committee takes into account the procedures

carried out by the control, following the visit of the CNPD agents, in order to comply with the
provisions of articles 38.1, 38.2 and 39.1 a) of the GDPR, as detailed in these letters
of November 21, 2019 and September 30, 2020. More specifically, it takes note of the facts
following:

- As to the breach of Article 38.1 of the GDPR providing for the obligation to involve the DPO to all questions relating to the protection of personal data, the restricted formation takes note that the local contact point has been appointed DPO of the audited body with effect from 1 October 2020.

However, the restricted training includes documents provided by the controlled that this newly appointed DPO performs his duties under the supervision of the DPO [of the group]. The Restricted Committee therefore wonders whether the newly appointed DPO is effectively associated with all data protection issues of a personal nature, and this in complete independence. Therefore, the CNPD is of the opinion that the auditee has not sufficiently demonstrated its compliance with article 38.1 of the GDPR and considers that it is necessary to pronounce an enforcement measure compliance in this regard.

- With regard to the violation of Article 38.2 of the GDPR providing for the obligation to provide the necessary resources to the DPO, the controlled states in its position paper of September 30, 2020 that the DPO newly appointed by Company A devotes 50% of his working time to data protection issues and that he is assisted by […] lawyers who devote […] so that there will be 1.5 FTE devoted to the protection of personal data.

In view of these elements, the Restricted Committee is of the opinion that the Chief's expectation investigation of 1 FTE or more is reached following the measures taken by the control course of the investigation. Consequently, the Restricted Committee considers that there is no instead of issuing a compliance measure in this respect.

- As for the violation of Article 39.1 a) of the GDPR relating to the mission of information and advice from the DPO to the controller, the controller exposes in its decision of position of September 30, 2020 the composition and functioning of the [Comité GDPR] which will allow the newly appointed DPO to inform and advise the

controller.

However, with regard to the documents provided by the controller, the restricted training understands that the DPO (previously local contact point, without having exercised the function of DPD) newly appointed by the audited person performs his duties under the supervision of the DPD [of the group], in such a way that it is not sufficiently demonstrated by the checked that the newly appointed DPO can effectively fulfill his mission information and advice to the controller of the controlled processing (Company A), and this independently. Consequently, the Restricted Committee considers that there is instead of issuing a compliance measure in this respect.

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

- to pronounce against the company "Company A" an administrative fine of one amount of eighteen thousand euros (18,000 euros) with regard to the violation of articles 38.1, 38.2 and 39.1. a) GDPR;
- to pronounce against the company "Company A" an injunction to put itself in compliance with Article 38.1 of the GDPR, within four months of the 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: ensure that the DPO is effectively involved in all questions relating to the protection personal data, and this independently;
- to pronounce against the company "Company A" an injunction to put itself in compliance with Article 39.1 a) 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:

ensure that the DPO can effectively fulfill his mission of information and advice to the person responsible for the controlled processing.

Thus decided in Belvaux on May 31, 2021.

For the National Commission for Data Protection sitting in restricted formation

Commissioner

Tine A. Larsen Thierry Lallemang

President

Marc Lemmer

Commissioner

Indication of remedies

This administrative decision may be 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.
