Decision of the National Commission sitting in restricted formation on

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

Deliberation no. 36FR/2021 of October 13, 2021

The National Commission for Data Protection sitting in restricted formation,

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

Lemmer, commissioners;

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

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

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

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

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

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

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

2;

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

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

its article 9;

Considering the following:

I.

Facts and procedure

1.

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

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

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

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

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

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

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

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

survey no.[…] conducted with Company A

(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 located at […], L-[…] and registered in the Trade and

Luxembourg companies under number B[…] (hereinafter: the “controlled”) and to designate Mr.

Christophe Buschmann as head of investigation. Said deliberation specifies that the investigation concerns

on the compliance of the control with section 4 of chapter 4 of the GDPR.

3.

According to article 3 of its articles of association, the controlled [aims to make, for it or for

third-party accounts, all insurance and co-insurance transactions in all branches

insurance other than life insurance] […].

4.

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

preliminary to the control to which the latter responded by letter dated October 5, 2018.

on-site visits took place on January 21 and May 23, 2019. Following these discussions, the Chief of investigation drew up audit report no.[…] (hereinafter: the “audit report”).

5.

It appears from the audit report that in order to verify the organization's compliance with the section 4 of chapter 4 of the GDPR, the head of investigation has defined eleven control objectives, to know :

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

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

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

4) Ensure that the DPO has sufficient expertise and skills to carry out its missions effectively;

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 11 November 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 appoint the DPO on the basis of his professional qualities2;

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

data3;

the obligation to provide the necessary resources to the DPO4;

the control mission of the DPD5.

8.

On August 10, 2020, the head of investigation sent an additional letter to the controller

to the statement of objections by which it informs the auditee of the corrective measures

that it proposes to the National Commission sitting in restricted formation (hereinafter: “the

“restricted formation”) to adopt. In this letter, the head of the investigation proposed to the restricted training to adopt 4 different corrective measures as well as to inflict on the controlled an administrative fine of 23,400 euros.

9.

By letter dated September 16, 2020, the person inspected sent the head of the investigation his comments on the additional letter to the statement of objections.

2 Objective 4

3 Goal 8

4 Objective 6

5 Goal #10

10.

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 investigation and the controller presented oral observations on the case and answered the questions posed by the Restricted Committee. The controller had the floor last.

II.

Place

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

1. On the principles

11.

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 […]”.

12.

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”.

13.

In addition, the Article 29 Data Protection Working Party has adopted on 13 December 2016 guidelines concerning DPOs which have been taken over and re-approved by the European Data Protection Board on May 25, 20186.

These guidelines specify that the level of expertise of the DPO “must be proportionate to the sensitivity, complexity and volume of data processed by an organization”7 and that “it It is necessary for DPOs to have expertise in the field of legislation and national and European data protection practices, as well as a in-depth knowledge of GDPR”8.

The DPO Guidelines go on to state that “[k]nowledge

14.

sector of activity and organization of the data controller is useful. The DPO should

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

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

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

---

also have a good understanding of the processing operations carried out,

as well as the information systems and the needs of the data controller in terms of

data protection and security".

2. In this case

15.

It appears from the audit report that, for the head of investigation to consider objective 4

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

DPD has at least three years of professional experience in data protection

data.

16.

According to the statement of objections, page 3, the DPO for control, a lawyer by training,

was absent for an extended period at the time of the audit, his return having been scheduled for

the beginning of 2020. It is specified that on the basis of the analysis of his CV, "the agents of

the CNPD were unable to identify any particular experience in terms of the protection of

data ". The statement of objections further states that "[b]ased on exchanges with

organization, the DPO had no particular expertise in the area of data protection.

given at the time of his appointment. The main criterion for his appointment to the post of

DPD served as his function as Chief Compliance & Legal Officer".

17.

The head of investigation then specifies that in the absence of the DPO, a deputy DPO provides the

duties of interim DPO, that the latter has "many years of experience

in the field of data protection and legal matters, as well as a long

experience in the sector of activity" and that he "can benefit, on request, from the assistance of a

person from the […] IT […] team".

18.

In his letter of September 16, 2020, the controller provides details as to

the professional experience of the DPO and maintains that the DPO had four years

experience in data protection at the time of the opening of the investigation.

The control specifies that the professional experience of the DPO could not be explained during

previous exchanges due to the prolonged absence of the DPO; he therefore could not have provided,

in 2019, that "his non-detailed and very succinct CV".

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

19.

Following the session of the restricted training of January 26, 2021, the control has

sent to the Restricted Committee, dated February 5, 2021, additional documents

concerning in particular the professional experience of the DPO. It appears that the DPD had

more than three years of experience in data protection at the time of

the opening of the investigation.

20.

The Restricted Committee notes that it is rightly stated on page 2 of the

statement of objections (under “preliminary remarks”) that “[t]he requirements of the GDPR

are not always strictly defined. In such a situation, it is up to the authorities to

control to verify the proportionality of the measures put in place by the persons in charge of

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

persons concerned. »

21.

However, the Restricted Committee notes that it is also specified on page 2 of the

statement of objections that the audited “has approximately […] employees and […] customers”. the
head of the investigation concludes that the person being audited processes a significant amount of data
personal. The Restricted Committee shares this assessment and considers that the expectation of the
head of investigation relating to the level of expertise of the DPO is proportionate to the volume of
processed data.

22.

The
Restricted Committee notes that
the details relating to
experience
of the DPO were provided by the controller only after he had been
sent the additional letter to the statement of objections; during his investigation,
head of investigation was therefore able to conclude that, on the basis of the information available to him, the existence
sufficient expertise adapted to the needs of the data controller in terms of
data protection could not be established. That being said, it should be noted that
the details provided by the controller in his letter of September 16, 2020 as well as the
additional documents sent to the restricted committee on February 5, 2021
allow to consider that, at the time of the opening of the investigation, the DPO had a
sufficient experience in data protection.

23.

In view of the foregoing, the Restricted Committee concludes that the breach of Article
37.5 GDPR does not exist.

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

the protection of personal data

1. On the principles

24.

According to Article 38.1 of the GDPR, the organization must ensure that the DPO is associated,

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

personal data.

25.

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”.

26.

The DPO Guidelines provide examples on how

to ensure this association of the DPO, such as:

-
-
-
-

invite the DPO to regularly attend management meetings

superior and intermediate;

to recommend the presence of the DPO when decisions having implications

with regard to data protection are taken;

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

to immediately consult the DPO when a data breach or other

incident occurs.

27.

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.

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

---

2. In this case

28.

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

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

DPD participates in a formal manner and on the basis of a frequency defined by the

management, project coordination committees, new product committees,

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

29.

According to the Statement of Objections, page 4, "[i]t appears from the investigation that no rule

or frequency has been defined as to the participation of the DPO or the Deputy DPO in the

Direction. The head of investigation further notes that the presence of the DPO or deputy DPO is not

not provided for in the “[…]” committee which meets before each launch of a new product.

Finally, the head of investigation notes that while measures aimed at better involving the DPO have been

proposed by the Deputy DPO to the Management Committee, the CNPD has not received confirmation that the DPD (or the Deputy DPO) participates in a formalized manner and on the basis of a frequency defined in Management Committee.

30.

In his letter of September 16, 2020, the controller indicates that after the end of the project internal implementation of the GDPR (end of January 2019), “it was agreed with the [Comité de management] that there would be passages or communications to the [Management Committee] when necessary” and specifies that “[i]t has not actually been fixed an automatic regularity” in adding that “however, we have not found a legal text explicitly imposing a specific regularity. The controller also communicated an inventory of the contacts between the DPD and the [Management Committee] for the period from February 1, 2019 to August 31, 2020. The audited further specifies that “Risk management” comes before the [Management Committee] several times a year in the context of "[...]" meetings and consults the DPO to prepare these meetings; this would be an additional channel of communication from the DPO to the [Committee of direction]. With regard to the Committee […], the auditee indicates that its procedure (including the latest version, communicated to the CNPD, is dated December 11, 2019) provides that the DPD “must intervene in the documentation of the product file which will be submitted during a meeting […] and give GDPR notice”. The controller then specifies that the DPO is "systematically involved prior to any launch of a new product or modified existing product”.

31.

It should be recalled that it has already been noted in point 20 of this decision that it

is rightly specified on page 2 of the statement of objections (under "remarks

preliminary") that "[t]he requirements of the GDPR are not always strictly defined. In

such a situation, it is up to the supervisory authorities to verify the proportionality of the measures

put in place by the data controllers with regard to the sensitivity of the data

processed and the risks incurred by the data subjects. »

32.

However, as mentioned in point 21 of this decision, the training

restricted shares the assessment of the head of investigation that the control processes a number

significant personal data. The Restricted Committee therefore considers that the

formalized and systematic participation of the DPO in relevant meetings, as it is

expected by the head of investigation, constitutes a proportionate measure to ensure

involving the DPO in all questions relating to the data protection of

personal.

33.

The Restricted Committee takes note of the fact that in its letter of September 16, 2020,

the inspected person indicates that "[t]he fixing of a regularity constituting a better guarantee of

collaboration, the [Management Committee] validated on September 16, 2020 the proposal of the

DPO to plan at least 4 visits per year to the [Management Committee] (…)". She takes

also notes that the procedure of the committee […] provides, at least since 11

December 2019, a verification step by the DPD for the launch of any new

product or for the modification of an existing product. However, the control specifies that the "DPO

was not a permanent member [of the Committee] […]and was not invited to meetings […]" and

indicates that "the [Executive Committee] has (…) decided [on] 16 September [2020] that the DPO would be

now a member [of the Committee] […]and would be systematically invited to meetings […]. »

34.

If these measures should facilitate the involvement of the DPO in all matters relating

to data protection, it should nevertheless be noted that these have been decided

under investigation. The Restricted Committee therefore considers that, at the start of the investigation, the

controller was unable to demonstrate that the DPO was associated with

appropriate manner to all questions relating to the protection of personal data.

35.

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

not respected by the controller.

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

1. On the principles

36.

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. »

37.

It follows from the DPO Guidelines that the following aspects should

in particular to be taken into consideration11:

- “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 ".

38.

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 significant. The data protection function must be effective and

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

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

---

2. In this case

39.

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

framework of this audit campaign, so that the head of investigation considers objective 6 as

completed by the person being controlled, he expects the person being controlled to have at least one ETP (equivalent time

full) for the data protection team. The chief investigator expects

also that the DPO has the possibility of relying on other services, such as the

legal department, IT, security, etc.

40.

In the statement of objections, page 4, the head of investigation indicates that "at the time

of the audit, the resources dedicated to the team in charge of data protection were

approximately 0.7 FTE, (0.3 for the Deputy DPO and 0.2 for each of the two lawyers in charge of

requests from data subjects). The Deputy DPD devotes around two-thirds of his

time in his duties as Tax & Legal Expert and cannot reduce this time for the benefit of the

Data protection. »

41.

The head of investigation also indicates "that it is expected that the DPD will resume his duties

beginning of 2020" noting that "the time that will be allocated to it in terms of protecting

data is not yet defined". As for the "deputy DPO", the head of investigation takes note of the

fact that he "can benefit, on request, from the help of a person from the […] IT team […]. »

42.

In his letter of September 16, 2020, the controller first confirms the

observations made by the head of the investigation: "It is true that at the precise moment of the 2nd day

audit, on May 23, 2019, due to exceptional circumstances, the resources were

temporarily limited for the legal/compliance and DP department and that the resource

usable overall in legal DP was 0.7 [FTE]. The controlled person then details the circumstances

which led to a limitation of the resources dedicated to the DPO as well as the

measures which have been decided upon in order to strengthen these resources.

43.

Finally, by email of March 12, 2021, the Restricted Committee was informed that the Committee

of the control department decided, on March 3, 2021, that the DPO will carry out its missions

full-time (one FTE) no later than the beginning of May 2021.

44.

The Restricted Committee takes note of the measures that have been decided by the control in course of investigation in order to strengthen the resources dedicated to the DPO and takes into account the fact that the particular circumstances which led to a limitation of the resources dedicated to the DPO at the start of the investigation were not foreseeable.

45.

In view of the foregoing, the Restricted Committee concludes that the breach of Article 38.2 GDPR does not exist.

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

1. On the principles

46.

According to Article 39.1. b) of the GDPR, the DPO has, among other things, the mission of “monitoring the compliance with this Regulation, other provisions of Union law or national law members with regard to data protection and the internal rules of the data controller processing or of the processor with regard to the protection of personal data, including including with regard to the distribution of responsibilities, awareness and training personnel involved in processing operations, and related audits”. the recital (97) clarifies that the DPO should help the body to verify compliance, at the level internal, GDPR.

47.

It follows from the DPO Guidelines12 that the DPO can, within the framework

of these control tasks, in particular:

~

collect information to identify processing activities;

~

analyze and verify the compliance of processing activities;

~

inform and advise the controller or processor and formulate

recommendations to him.

2. In this case

48.

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 formalized data protection control plan

(even if not yet executed)”.

49.

According to the Statement of Objections, p. 5, “[i]t appears from the investigation that the organization

does not have a control plan. The head of investigation specifies that the deputy DPD indicated "that

the follow-up of requests from data subjects is already operational, in particular via a

regular monitoring of the deadlines for access requests”. The head of the investigation further notes that “that

the Deputy DPO issues opinions and recommendations" and that "the Group Data Protection has carried out

12 WP 243 v.01, version revised and adopted on April 5, 2017, p. 20

two audits within […] Company A in January and October 2018.” The head of investigation
nevertheless notes that "the monitoring plan relating to data protection was in
under construction at the time of the audit. »

50.

In his letter of September 16, 2020, the controller indicates that the audit mentioned by the
CNPD “concerned the assessment of the GDPR implementation project and aimed to ensure that
[the controlled] properly and fully fulfills its obligations [relating to the protection of
data] ". He specifies that “[t]here has been regular monitoring by the Group Audit of the points still open
or to be improved and therefore exchanges between the DPO and the group". The controller still says
that a “DPO Committee has been created within the Group” made up of “the Group DPO and the
DPO of the various businesses within the EU, including Luxembourg”. According to the control,
It is a “control and information exchange tool”. Finally, he notes that "we
we also understand that it is important, apart from monitoring the group audit, that the DPO
has a monitoring or control plan” before specifying that such a control plan
was established and “approved by the [Management Committee] at its meeting of September 16, 2020”.
This inspection plan was communicated by the inspected party as an appendix to its letter of 16
September 2020.

51.

The Restricted Committee notes that Article 39.1 of the GDPR lists the missions that
the DPO 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
DPD can fulfill its control mission. DPO Guidelines
indicate in particular that the keeping of the register of processing activities referred to in Article 30 of the
GDPR can be entrusted to the DPO and that “[t]his register should be considered as one of the
tools allowing the DPO to carry out its missions of monitoring compliance with the GDPR as well as

information and advice from the controller or processor.13”

52.

It appears from the investigation file that at the time of the on-site visit of January 21, 2019,

the processing register was kept by the Deputy DPO14. The restricted formation falls under

nevertheless that this element taken in isolation is not sufficient to demonstrate that the control mission

compliance with the GDPR was carried out in an adequate manner.

53.

The Restricted Committee recalls that it has noted in point 20 of this decision

that it is rightly stated on page 2 of the statement of objections (under “remarks

13 WP 243 v.01, version revised and adopted on April 5, 2017, p. 22

14 Minutes of the visit of January 21, 2019, page 2

preliminary”) that “[t]he requirements of the GDPR are not always strictly defined.

In such a situation, it is up to the supervisory authorities to verify the proportionality of the

measures put in place by the data controllers with regard to the sensitivity of the

data processed and the risks incurred by the persons concerned. »

54.

However, as mentioned in point 21 of this decision, the training

restricted shares the assessment of the head of investigation that the control processes a number

significant personal data.

55.

The Restricted Committee therefore considers that the inspection mission carried out

by the DPO to the auditee should be sufficiently formalized, for example by a plan

data protection control, in order to be able to demonstrate that the DPO

carries out its mission of monitoring compliance with the GDPR in an adequate manner.

56.

The Restricted Committee takes note of the control plan communicated by the

checked in the appendix to his letter of September 16, 2020.

57.

Nevertheless, the Restricted Committee observes that this control plan was drawn up after

the start of the investigation and therefore considers that at the start of the investigation, the person checked was not

able to demonstrate that the DPO carries out its tasks of monitoring compliance with the GDPR

in a way that suits their needs.

58.

In view of the foregoing, the Restricted Committee concludes that Article 39.1. b) GDPR

was not respected by the controller.

III.

On the corrective measures and the fine

A. Principles

59.

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 operations of

envisaged processing are likely to violate the provisions of this

settlement;

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

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

settlement;

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

submitted by the data subject with a view to exercising their rights under this

this Regulation;

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

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

specifically and within a specified time;

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

personal data breach;

f)

impose a temporary or permanent limitation, including a ban, on the

treatment;

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

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

measures to the recipients to whom the personal data have been

disclosed pursuant to Article 17(2) and Article 19;

(h) withdraw a certification or order the certification body to withdraw a

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

certification not to issue certification if the requirements applicable to the

certification are not or no longer satisfied;

i)

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

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

specific to each case;

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

third country or an international organisation. »

60.

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

the purpose of the processing concerned, as well as the number of data subjects

affected and the level of damage they suffered;

b) whether the breach was committed willfully or negligently;

c) any action taken by the controller or processor to mitigate the

damage suffered by the persons concerned;

d) the degree of responsibility of the controller or processor, account

given the technical and organizational measures they have implemented under the

sections 25 and 32;

e) any relevant breach previously committed by the controller or

the subcontractor ;

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

and to mitigate any negative effects;

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

h) the manner in which the supervisory authority became aware of the breach, in particular whether,

and the extent to which the controller or processor 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, as a result of the breach".

61.

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.

62.

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

with the GDPR during the investigation process or to remedy 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

63.

In its supplementary letter to the statement of objections of 10 August 2020, the

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

administrative fine in the amount of 23,400 euros.

64.

In order to decide whether to impose an administrative fine and to decide, if

applicable, of the amount of this fine, the Restricted Committee analyzes the criteria laid down by

GDPR Article 83.2:

- As to the nature and gravity of the breach [Article 83.2 a) of the GDPR], with regard to

breaches of Articles 38.1 and 39.1.b) of the GDPR, the Restricted Committee 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 case where the DPO is involved from the stage on

as early as possible to all questions relating to data protection and exercises

its missions effectively, in particular the mission of monitoring compliance with the GDPR.

- As for the duration criterion [article 83.2.a) of the GDPR], the restricted training falls under:

(1) That it was decided by the control, in September 2020, to take measures

adapted to facilitate the involvement of the DPO in all questions relating to the

Data protection. The breach of Article 38.1 of the GDPR therefore lasted in the

time, at least between May 25, 2018 and September 2020;

(2) That an inspection plan was communicated to the CNPD by the inspected party on 16

September 2020 and that this plan has been approved by the Control Management Committee on the same date. The breach of Article 39.1.b) of the GDPR therefore lasted for the time, at least between May 25, 2018 and September 16, 2020;

- 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 audit deals with special categories of personal data, namely data concerning health.

65.

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.

66.

The Restricted Committee notes that if several measures have been decided by the control in order to remedy the shortcomings, these were not decided until after the launch of the investigation by CNPD officials dated 17 September 2018 (see also point 61 of this decision).

67.

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 and 39.1.b) of the GDPR.

68.

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 and 39.1.b) of the GDPR is alleged at the time of the inspection, the maximum amount of the fine that can be withheld is 10 million

euros or 2% of worldwide annual turnover, whichever is higher.

69.

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 13,200 euros appears

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

---

2. Regarding the taking of corrective measures

70.

In its supplementary letter to the statement of objections of 10 August 2020, the

head of investigation proposes to the restricted committee to take corrective measures

following:

"a) Order the implementation of measures allowing the DPO (or a team "

Data Protection "dedicated) to acquire sufficient expertise adapted to the needs

of the data controller in terms of data protection in accordance with the

provisions of Article 37, paragraph (5) of the GDPR and the guidelines relating

to the DPO of the "article 29" working party on data protection which specifies

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

and the volume of data processed by the organization. Several ways can be

considered to achieve this result:

- provide internal or external support to your DPO on specific legislation

in personal data protection and system security

of information ;

- enroll your DPO in accelerated/intensive training in the subjects listed above

above mentioned;

- designate another DPO who has sufficient expertise.

b) Order the implementation of measures allowing the DPO to be associated with all

data protection issues, 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 could be to analyze,

with the DPO, all relevant committees/working groups with regard to the protection

data and formalize the terms of its intervention (previous information

meeting agenda, invitation, frequency, permanent member status, etc.).

c) Order the provision of necessary resources to the DPO in accordance with

the requirements of Article 38 paragraph 2 of the GDPR. Although several ways

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

to relieve the DPO of all or part of his other missions/functions and/or of him

provide formal support, internally or externally, for the exercise of its missions

from DPD.

---

d) Order the deployment of the control mission, in accordance with article 39

paragraph 1 b) of the GDPR. Although several ways can be envisaged to

achieve this result, the DPO should document its controls on the application of

internal data protection rules and procedures (second line

defence). This documentation could take the form of a control plan. »

71.

As for the corrective measures proposed by the head of investigation under a) and under c) of the

point 70 of this decision, the breaches of Articles 37.5 and 38.2 of the GDPR not being constituted, there is no need to examine the related corrective measures.

72.

As for the other corrective measures proposed by the head of investigation and by reference to point 62 of this Decision, the Restricted Committee takes into account the steps taken by the controller to comply with the provisions of articles 38.1 and 39.1.b) of the GDPR, in particular the measures described in its letter of September 16 2020. More specifically, it takes note of the following facts:

- With regard to the violation of Article 38.1 of the GDPR, the Restricted Committee finds that it has been decided by the auditee to take appropriate measures to facilitate involving the DPO in all matters relating to data protection. The Restricted Committee therefore considers that there is no need to pronounce the measure correction proposed by the head of investigation under b) of point 70 of this decision.
- With regard to the violation of Article 39.1.b) of the GDPR, the restricted training notes that a control plan was communicated to the CNPD by the control on the date of September 16, 2020 and that this plan has been approved by the Control Management Committee at the same date. The Restricted Committee therefore considers that there is no need to pronounce the corrective action proposed by the head of investigation under d) of point 70 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 38.1 and 39.1.b) of the GDPR;

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

one thousand two hundred euros (13,200 euros) with regard to the violation of articles 38.1 and 39.1.b) of the

GDPR.

Thus decided in Belvaux on October 13, 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.
