Decision of the National Commission sitting in restricted formation on

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

Deliberation No. 41FR/2021 of October 27, 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 […], […] and registered in the Trade and

Luxembourg companies under the number[…] (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 subject of control is all activities relating to banks or establishments

credit […].

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 September 28, 2018.

on-site visit took place on January 29, 2019. Following these exchanges, the head of investigation established

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 October 21, 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 publish the contact details of the DPO2;

the obligation to involve the DPO in all questions relating to the protection of data3;

the obligation to guarantee the autonomy of the DPO4;

the control mission of the DPD5.

8.

By letter dated November 15, 2019, the controller sent the head of the investigation his decision position on the failings noted in the statement of objections.

9.

On August 3, 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 it proposes to the National Commission sitting in restricted formation (hereafter: the restricted") to adopt. In this letter, the head of investigation proposed to the restricted formation to adopt 4 different corrective measures as well as to impose a fine on the controlled person administrative in the amount of 18,700 euros.

2 Objective 2

3 Goal 8

4 Objective 7

5 Goal #10

Decision of the National Commission sitting in restricted formation on the outcome of survey no.[…] conducted with Company A

10.

By letter dated September 8, 2020, the person inspected sent the head of the investigation his comments on the additional letter to the statement of objections.

The case was on the agenda of the restricted committee meeting of May 31, 2021.

11.

In accordance with Article 10.2. b) the internal regulations of the National Commission, the head of investigation and the control presented oral observations on the case and responded to the questions posed by the Restricted Committee. The controller spoke last.

II.

Place

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

1. On the principles

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

12.

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

data subjects must be able to contact the DPO about all

questions relating to the processing of their personal data and the exercise of

their rights under the GDPR.

13.

The DPO Guidelines explain in this regard that this requirement

aims to ensure that “those concerned (both inside and outside the

body) can easily and directly contact the DPO without having to

go to another department of the organization”. The guidelines also state that

“the contact details of the DPO must contain information allowing persons

concerned to reach it easily (a postal address, a telephone number

specific address and/or a specific e-mail address)”.6

14.

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

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

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

understandable and easily accessible, in clear and simple terms. From

information that must be transmitted to the person concerned includes information relating to

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

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

---

2. In this case

15.

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

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

the organization publishes the contact details of its DPO internally within the organization and

external to the public. The DPO must be easily and directly contactable via a

communication channel adapted to the persons concerned. As part of this campaign

audit, active internal communication is expected, in particular via emails,

newsletters, dedicated spaces on the intranet. Externally, it is at least expected that the

contact details of the DPO are easily accessible on the body's website.

16.

According to the Statement of Objections, page 2: “The investigation shows that the website

Company A's public does not provide direct contact details for the DPO. In case of questions

or requests from data subjects, the website provides a form to

complete and return to a generic email address ([…]) or by post to the address of the

hotline […] or via […] secure messaging. »

17.

The head of the investigation concludes that "the persons concerned external to Company A

cannot contact the DPO directly without having to contact another

service of the organization. »

18.

In its position paper of November 15, 2019, the auditee does not question the

findings made by the head of investigation and indicates that following the breach found,

a

address

E-mail

dedicated

has

summer

created

" in order to

that

them

data subjects can contact the Data Protection Officer directly

(“DPD”). The control then specifies where the contact details of the DPO have been published, namely

on its website as well as in its data processing policy

personal.

19.

During the meeting of May 31, 2021, the Restricted Committee noted that the contact details

of the DPO were not mentioned in the section of the website of the controller relating to

the exercise of the rights of data subjects nor in the form found under this

section and asked the controller for additional information in this regard. By email from 4

June 2021, the controller informed the restricted committee of the mention of the contact details of the DPO

in this section as well as in the said form.

20.

If measures have been taken by the auditee to comply with the obligation to

publication of the contact details of its DPO, it should be noted that these were decided

only under investigation. The Restricted Committee notes that at the start of the investigation, the

audited had not published the contact details of its DPO.

21.

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

not respected by the controller.

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

22.

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.

23.

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”.

24.

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;

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

---

to immediately consult the DPO when a data breach or other

incident occurs.

25.

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

26.

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.

27.

According to the Statement of Objections, page 3, “[i]t appears from the investigation that the DPO

intervenes by invitation or on an ad hoc basis at various internal meetings or committees

which are discussed the issues or projects with impacts in terms of

data protection, but there is no set rule or frequency as to the

participation of the DPO in these committees. The head of investigation then notes that "[t]he fact that the

DPD took part in two Internal Control Committee meetings (January 2019 and August 2018),

Management Board of November 2017, that he be a permanent guest of the Safety Committee and

that he be involved if a Data Protection aspect concerning a new product is not sufficient to

demonstrate the formal, permanent and regular nature of the involvement of the DPO. »

28.

In its position paper of November 15, 2019, the controller indicates that the DPD is

spoke on an ad hoc basis in September 2019 to the “Internal Control Committee” and to the

" Executive Committee ". He then indicates that a "quarterly intervention at the Control Committee

Internal will be implemented and formalized” in its “Data Protection Policy

personal”.

29.

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. »

30.

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. Leader investigation concludes that the auditee processes a significant amount of personal data. The Restricted Committee shares this assessment and therefore considers that the participation formalized and systematic from the DPO at the relevant meetings, as expected by the head of investigation, constitutes a proportionate measure to ensure the association of the DPO with all questions relating to the protection of personal data.

31.

The Restricted Committee takes note of the fact that in its response of 8 September 2020 in the additional letter to the statement of objections, the controller provided "elements additional information (…) in order to respond to the corrective measures proposed by the head of investigation", concerning in particular the association of the DPO in all questions relating to data protection. The controller provided a list of 6 committees (concerning areas of IT, risk management and outsourcing) of which the DPO is a member as well as indications on the interventions/participations of the DPO in other committees and meetings (i.e. the "[…] Committee", the "[…]" meetings and the Oversight Committee internal "in order to present the quarterly activity report or any other subject that it deems necessary ").

32.

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.

33.

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 breach of the obligation to guarantee the autonomy of the DPO

1. On the principles

34.

Under Article 38.3 of the GDPR, the organization must ensure that the DPO “not

receive any instructions with regard to the exercise of the missions". Furthermore, the DPO

“reports directly to the highest level of management” of the organization.

35.

Recital (97) of the GDPR further states that DPOs “should be able

to exercise their functions and missions in full independence”.

36.

According to the DPO Guidelines8, Article 38.3 of the GDPR “provides

certain basic safeguards intended to ensure that DPOs are able to exercise

their missions with a sufficient degree of autonomy within their organization. […] That

means that, in the exercise of their tasks under Article 39, DPOs must not

receive instructions on how to handle a case, for example, what outcome should be

obtained, how to investigate a complaint or whether to consult the supervisory authority.

Furthermore, they cannot be required to adopt a certain point of view on a matter related to the

data protection legislation, for example, a particular interpretation

law. […] If the controller or processor makes decisions that are

incompatible with the GDPR and the opinion of the DPO, the latter should have the possibility to indicate

clearly his opinion diverges at the highest level of management and to decision makers. In this

In this respect, Article 38(3) provides that the DPO “reports directly to the level most

higher than the management of the controller or the processor". Such a surrender direct account ensures that senior management (e.g. board of directors) has knowledge of the opinions and recommendations of the DPO which are part of the mission of the latter consisting in informing and advising the data controller or the subcontracting. The preparation of an annual report on the activities of the DPO intended for the management is another example of direct accountability. »

2. In this case

37.

It appears from the audit report that, for the head of investigation to consider objective 7 as completed by the auditee as part of this audit campaign, he expects the DPD is "attached to the highest level of management in order to guarantee its autonomy".

8 WP 243 v.01, version revised and adopted on April 5, 2017, p. 17 and 18

38.

According to the statement of objections, page 4, "During the investigation, the officers of the CNPD noted the existence of several hierarchical intermediaries between the DPO and the Direction. Indeed, the DPO is attached to a person from the "[...]" department who is herself even attached to a person from the "[...]" department who is himself attached to the Chief Compliance Officer. Although the DPO can intervene on an ad hoc basis in the Executive Committee and to the Internal Control Committee at its request and at any time, the reporting line to the Management and therefore access to the latter are not direct and permanent. »

39.

In his letter of September 8, 2020, the controller indicates that in order to guarantee the autonomy of the DPO: “i. the function of DPO has been hierarchically attached to the Chief Group Compliance Officer (CCO) From January 15, 2020. ii. The CCO is invited member of the Executive Committee of Company A since October 1, 2018 (no intermediary hierarchy between the DPO and the highest level of Management) and reports directly to the Chief Executive Officer, as well as to the Chairman of the Board of Directors. iii. A report quarterly activity report on data protection is presented by the DPO to […] composed part of the Executive Committee). » The audit further indicates that meetings weekly meetings are organized between the DPO and the CCO.

40.

If it does not follow from the provisions of the GDPR that the DPO must necessarily be attached to the highest level of management in order to guarantee its autonomy, the training nevertheless recalls that it has noted in point 29 of this decision that it is correctly stated on page 2 of the statement of objections (under "preliminary remarks) that “[t]he GDPR requirements are not always strictly defined. In such situation, it is up to the supervisory authorities to verify the proportionality of the measures put in place by data controllers with regard to the sensitivity of the data processed and the risks incurred by the persons concerned. »

41.

However, as mentioned in point 30 of this decision, the training management shares the assessment of the head of investigation, mentioned on page 2 of the statement of objections, according to which the controller processes a significant amount of data personal. The Restricted Committee therefore considers that, in the absence of other measures which would make it possible to demonstrate that direct reporting to the highest level management is formalized, the hierarchical attachment of the DPO to the highest level of the management, as expected by the head of investigation, constitutes a proportionate measure in order to

guarantee its autonomy.

42.

In this regard, the Restricted Committee notes that at the time of the opening of the investigation, the DPO was not attached to the highest level of management and has not been demonstrated by the controller than direct reporting to the highest level of management was formalized.

43.

In view of the foregoing, the Restricted Committee concludes that Article 38.3 of the GDPR has no not respected by the controller.

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

1. On the principles

44.

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.

45.

It follows from the DPO Guidelines9 that the DPO may, 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

46.

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)”.

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

47.

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

does not have a control plan. Although the organization has informed the CNPD that controls

relating to data protection are under construction, that they will be integrated into

the Compliance Monitoring program and that recourse to external assistance is envisaged

to build this monitoring program, the organization did not carry out the missions of

control at the time of the survey. »

48.

In his letter of September 8, 2020, the controller indicates that he "asked the help of

consultants for the development of a control plan […]" and that "[t]his [plan] was finalized in

[d]ecember 2019 and is applicable in 2020". The control further indicates that in "April 2019

Internal Audit [of the controlled] (3rd line of defence) carried out a mission on the implementation

of Regulation (EU) 2016/679 which gave rise to recommendations. » The precise control

also that "checks have been carried out or are in the process of being carried out by the DPO",

in particular the review of the processing register and the review of the contractual clauses relating

to data protection. Finally, the controller indicates that "in accordance with article 25 of the

regulation, the principles of "data protection by design and data protection

default data" have been implemented as an a priori control for the implementation of

new processing of personal data. »

49.

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 tasks of monitoring compliance with the GDPR as well as

information and advice from the controller or processor.10"

50.

It appears from the answers of the control to the preliminary questionnaire that, from the beginning of

investigation, the DPO had the task of "coordinating the documentation of the processing operations in the

register »11. The Restricted Committee nevertheless notes that this element taken in isolation is not sufficient not have to demonstrate that the task of monitoring compliance with the GDPR could have been carried out adequately.

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

11 Audit response of 09/28/2018 to the preliminary questionnaire (question 5.d).

51.

The Restricted Committee recalls that it has noted in point 29 of this decision that it is rightly stated 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 persons concerned. »

52.

However, as mentioned in point 30 of this decision, the training management shares the assessment of the head of investigation, mentioned on page 2 of the statement of objections, according to which the controller processes a significant amount of data personal.

53.

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

54.

The Restricted Committee takes note of the elements communicated by the controller in its letter of September 8, 2020 concerning the development of a control plan finalized in December 2019 and its application in 2020.

55.

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.

56.

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

57.

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. »

58.

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".

59.

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.

60.

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

61.

In its supplementary letter to the statement of objections of 3 August 2020, the

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

administrative fine in the amount of 18,700 euros.

62.

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, 38.3, and 39.1.b) of the GDPR, restricted training

notes that the appointment of a DPO by an organization cannot be efficient and effective, except

know how 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 in order to be able to

liaise with the DPO regarding all matters relating to the processing of their

personal data and the exercise of their rights, where the DPO is associated from the

earliest possible stage in all questions relating to data protection,

can carry out its functions and missions in complete independence, and can exercise

effective in its missions, 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 the auditee indicated in its statement of November 15, 2019 that a

dedicated email address has been created “so that data subjects can

contact the Data Protection Officer directly" and that the contact details
of the DPO have been published on its website as well as in its privacy policy.
processing of personal data. The breach of Article 37.7 of the GDPR therefore
lasted in time, at least between May 25, 2018 and November 2019.
(2) That it has been decided by the auditee to take appropriate measures to facilitate
involving the DPO in all matters relating to data protection,
which are described in his letter of September 8, 2020. The failure to
article 38.1 of the GDPR therefore lasted over time, at least between May 25, 2018
and September 2020;
(3) That the elements communicated by the control during the investigation, and in particular
by email of June 4, 2021 following the meeting of May 31, 2021, do not allow
demonstrate that the DPO would be able to report directly to the highest
management level in a formalized manner. Breach of Article 38.3 of the GDPR
therefore lasted over time, from May 25, 2018, it being specified that the training
has not been able to ascertain that the breach has ended;
(4) That a control plan was finalized in December 2019 and applied in 2020. The
breach of Article 39.1.b) of the GDPR therefore lasted over time, at the very least
between May 25, 2018 and December 2019.
63.
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.
64.
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 59 of

this decision).

65.

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 37.7, 38.1, 38.3 and 39.1.b) of the GDPR.

66.

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. To the extent that a breach of Articles 37.7, 38.1, 38.3, and 39.1(b) 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.

67.

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 18,700 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

68.

In its supplementary letter to the statement of objections of 3 August 2020, the
head of investigation proposes to the restricted committee to take corrective measures
following:

“a) Order the publication of the contact details of the Data Protection Officer

in accordance with the requirements of Article 37 paragraph 7 of the GDPR and the lines

DPO Guidelines of the Article 29 Working Party on Data Protection

data indicating that data subjects should be able to easily and easily

contact the DPO directly without having to go to another service

the organism. Thus, one of the ways to achieve this result would be to publish the

contact details of the DPO on the public website of [Company A] insofar as this does not

would not already be done.

b) Order the implementation of measures ensuring the association of the DPO 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

with the meeting agenda, invitation, frequency, permanent member status,

etc....).

---

c) Order the establishment of a mechanism guaranteeing the autonomy of the DPO

in accordance with the requirements of Article 38 paragraph 3 of the GDPR. Several

measures can be considered to achieve this result, such as

attachment of the DPO to the highest level of management in order to guarantee as much as possible

its autonomy or the creation of a formalized and regular line of direct reporting,

as well as an emergency escalation mechanism at the steering to bypass

the intermediate hierarchical level(s).

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

paragraph 1 b) of the GDPR. The DPO should therefore document its controls relating to

application of internal data protection rules and procedures

(second line of defense). This documentation could take the form of a plan

control insofar as it has not already been done.

69.

As for the corrective measures proposed by the head of investigation and with reference to the

point 60 of this decision, the Restricted Committee takes into account the procedures

carried out by the controlled in order to comply with the provisions of articles 37.7, 38.1, 38.3,

and 39.1.b) of the GDPR, in particular the measures described in its letter of November 15, 2019

and in its letter of September 8, 2020. More specifically, it takes note of the facts

following:

- With regard to the violation of Article 37.7 of the GDPR, the Restricted Committee finds

that a dedicated email address has been created and that the contact details of the DPO have been published

on the website of the controlled as well as in its policy regarding the processing of

personal data. The Restricted Committee therefore considers that there is no need to

pronounce the corrective measure proposed by the head of investigation under a) of point 68 of the

this decision.

- 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

corrective action proposed by the head of investigation under b) of point 68 of this decision.

- With regard to the violation of Article 38.3 of the GDPR, the Restricted Committee finds

that the elements communicated by the audit during the investigation, and in particular by

email of June 4, 2021 following the meeting of May 31, 2021, do not demonstrate

---

that the DPO would be able to report directly to the highest level of the
management in a formal way. The Restricted Committee therefore considers that there is reason to
pronounce the corrective measure proposed by the head of investigation under c) of point 68 of the
this decision.

- With regard to the violation of Article 39.1.b) of the GDPR, the restricted training falls
that a control plan was finalized in December 2019 and applied in 2020. Training
restricted therefore considers that there is no need to pronounce the corrective measure
proposed by the head of investigation under d) of point 68 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, 38.3 and 39.1.b) of the GDPR;
- to impose an administrative fine on Company A in the amount of ten-
eight thousand seven hundred euros (18,700 euros) with regard to the violation of articles 37.7, 38.1, 38.3
and 39.1.b) GDPR;
- issue against Company A an injunction to comply with the
Article 38.3 of the GDPR within four months of notification of the decision of the
restricted training, in particular:
ensure the establishment and maintenance of a formal mechanism guaranteeing the autonomy
of the DPD.

Thus decided in Belvaux on October 27, 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.
