Decision of the National Commission sitting in restricted formation on

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

Deliberation n° 20FR/2021 of June 11, 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:

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

Survey No. […] conducted with Company A

I.

Facts and procedure

1. Considering 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

pursuant to 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 and on the free movement of such data, and repealing the Directive 95/46/EC (General Data Protection Regulation) (hereinafter: the " GDPR"), the National Data Protection Commission (hereinafter: the "National Commission" or the "CNPD") has decided to launch an investigation campaign thematic on the function of the DPO. Thus, 25 audit procedures were opened in 2018, concerning both the private and public sectors.

2. In particular, the National Commission decided by deliberation No. […] of 14 September 2018 to open an investigation in the form of a data protection audit with Company A established at […] L- […] and registered in the trade and companies register 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 auditee [is active in the field of transport] […].

4. The control has approximately […] employees and in terms of its activities […].

5. 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 9, 2018. on-site visits took place on February 4 and May 2, 2019. Following these discussions, the Chief investigation drew up audit report No. […] (hereinafter: the "audit report").

6. It appears from the audit report that in order to verify the compliance of the organization with the section 4 of Chapter 4 of the GDPR, the head of investigation has defined eleven control objectives, namely:

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

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) 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.

7. By letter dated 7 November 2019 (hereinafter: the “statement of objections”), the head
of investigation informed the control of the breaches of the obligations provided for by the GDPR
which he found during his investigation. The audit report was attached to that letter.

8. 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 data2;

the obligation to guarantee the autonomy of the DPO3;

the control mission of the DPD4;

the information and advice mission of the DPO5.

~

~

~

9. By letter dated December 4, 2019, the inspector sent the head of investigation his decision

position on the shortcomings noted in the statement of objections.

2 Goal 8

3 Objective 7

4 Goal #10

5 Goal #9

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

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

grievances”) by which he informs the controlled party of the corrective measures and the fine

administrative structure that it proposes to the National Commission sitting in restricted formation (here

after: the “restricted formation”) to adopt. In this letter, the head of investigation proposed

the Restricted Committee to adopt three different corrective measures, as well as to impose

to the control an administrative fine of 15,000 euros.

11. By letter dated September 17, 2020, the person inspected sent the head of investigation his

comments on the additional letter to the statement of objections.

12. The case was on the agenda of the Restricted Committee meeting of 13 November

2020. In accordance with Article 10.2. b) the internal rules of the Commission

national, the head of investigation and the controller presented their oral observations in support

their written observations and answered the questions posed by the Panel

restraint. The controller spoke last.

II.

Place

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

the protection of personal data

1. On the principles

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

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

personal data.

14. 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 GDPR compliance and encourage a grounded approach

on data protection by design; it should therefore be a procedure

customary in 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 groups

of work dedicated to data processing activities within the organisation”6.

15. 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.

16. 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

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

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

participates in a formalized manner and on the basis of a 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.

18. According to the Statement of Objections, page 3, “the DPO participates in the Board of Directors on invitation or on request, but not in a systematic way (…) The participation of the DPO to project meetings with an impact on data protection is planned, but not still systematically in place. The Statement of Objections then states that "The fact that the intervention of the DPO in the various meetings relevant to the with regard to the protection of personal data is not systematic is not of such as to guarantee appropriate involvement of the DPO, nor to establish its position in as an interlocutor within the organization. »

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

---

19. In addition, the head of investigation, taking into consideration the protection policy data which, during the investigation, was being compiled by the controller, falls in the statement of objections, page 3, that "if the existence of a protection policy data specifying the need to integrate the DPO in all matters related to the data protection is an important element of governance, it is not enough to ensure appropriate and timely involvement of the DPO at operational level. Of the internal procedures specifying in concrete terms how the DPO must be involved, the systematic invitation of the DPO to meetings or his appointment as permanent member of a committee would, for example, be elements allowing demonstrate its operational involvement. »

20. In its statement of December 4, 2019, page 2, the auditee indicates that “[i]t is important (…) to take into account the particularities of each organization as well as its decision-making and organizational functioning in order to assess in what "way

appropriate” the controller, together with the processor, must associate the DPO “with all matters relating to data protection”” and maintains that “Neither the GDPR, nor do the Guidelines provide for an obligation for the controller to make the DPO a permanent member of any decision-making committee”. Also, according to the audited “the requirement formulated in the report that the DPO be a member of the Committee of Directors […] is neither in conformity with these texts, nor necessary to the performance of the tasks of the DPO. »

21. The auditee also recalls that measures have been taken “in order to help the DPO to carry out its missions", including by appointing for each service, "one or more “GDPR correspondents” whose missions are in particular to relay the objectives of the data protection policy within their department and to coordinate operations compliance under the responsibility of the department head concerned and the DPO. They have direct access to it. »

22. The Restricted Committee notes that the GDPR does not specify which measures are should be taken by the data controller to ensure the association of the DPO to all questions relating to data protection. As for the guidelines concerning the DPOs, these formulate recommendations and best practices, in order to guide data controllers in complying with their

governance, including providing examples of how to ensure this association.

23. Nevertheless, 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
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. »

24. In this respect, the Restricted Committee observes that the audited counts approximately […]
employees (according to the investigation file), that it has an internal service of […].
[…]. It nevertheless follows that the activities of the controlled involve data processing.
personal data which potentially affects a significant number of
persons concerned. However, if the control has put in place, prior to the start of
the investigation, certain organizational measures facilitating the association of the DPO,
in particular by appointing "GDPR correspondents" for each service, the training
nevertheless considers that the formalized and systematic participation of the DPO
at relevant meetings, as expected by the head of investigation, is a measure
proportionate in order to ensure the association of the DPO in all matters relating to the
Protection of personal data.

25. The Restricted Committee takes note of the fact that in its letter of 17 September 2020, the
controlled indicates that it was decided to “formalize monthly meetings between the DPO
and department heads who process the most personal data (mainly
IT, human resources and […]) (…) as well as biannual meetings with
the other heads of departments” and to add “as an appendix to the general management policy
of data, a sheet allowing each person in charge of a project to deal with
the DPO the issue of data protection”. If these measures should allow
to ensure the association of the DPO in all questions relating to data protection,
it should be noted that these were decided during the investigation by the person inspected.
The Restricted Committee therefore agrees with the finding of the head of investigation that,
at the start of the investigation, the controller was unable to demonstrate that the DPO was

appropriately associated with all data protection issues

personal.

---

26. The Restricted Committee also notes that it does not have the documentation that

would make it possible to demonstrate that such measures have been taken by the person being controlled.

27. In view of the foregoing, the Restricted Committee concludes that Article 38.1 of the GDPR has not

been complied with by the controller.

B. On the breach of the obligation to guarantee the autonomy of the DPO

1. On the principles

28. According to Article 38.3 of the GDPR, the organization must ensure that the DPO “receives no

no instructions with regard to the exercise of the missions”. Furthermore, the DPD "does

report directly to the highest level of management” of the organization.

29. Recital (97) GDPR further states that DPOs “should be able to

to exercise their functions and missions in full independence”.

30. According to the DPO Guidelines7, Article 38.3 of the GDPR “provides for 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

be obtained, how to investigate a complaint or whether to consult the authority of

control. Moreover, they cannot be required to adopt a certain point of view on a

question relating to data protection legislation, for example, a

particular interpretation of the law. […] If the controller or processor

makes decisions that are incompatible with the GDPR and the opinion of the DPO, the latter should be given the opportunity to clearly state their dissent at the highest level management and decision makers. In this regard, Article 38(3) provides that the DPD "reports directly to the highest level of management of the Head of processor or processor". Such direct accountability ensures that senior management (e.g. the board of directors) is aware of the opinions and recommendations of the DPO that fall within the scope of the latter's mission

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

---

consisting of informing and advising the controller or processor.

The preparation of an annual report on the activities of the DPO intended for the highest level management is another example of direct accountability. »

2. In this case

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

32. According to the statement of objections, page 3, ""It appears from the investigation that the […] indicates that the DPO reports directly to the highest level of the Company, in this case the Board of Directors and the General Management. However, Company A [was] not in able to demonstrate the existence of such a direct relationship at the highest level of the management, for example, through an activity report. Regarding the connection Hierarchical, the DPO was initially attached to the Legal Director, himself attached

to the administrative and financial director. »

33. With regard to the preparation of an activity report, the head of investigation is responsible on page 4 of the statement of objections that a modification took place during the investigation in the sense of compliance, the DPO now establishing a monthly report for the attention of the Director General. The head of investigation notes, however, that the DPO should be able to independently determine the content of this monthly report which is first and foremost discussed with the Administrative and Financial Director.

34. With regard to the hierarchical attachment, the head of investigation recalls on page 4 of statement of objections that "the existence of several hierarchical levels between the DPD and the highest level of management is not such as to guarantee its autonomy. ” and underlines that during the investigation, the control indicated “that the attachment hierarchy of the new DPD was uncertain".

35. In its statement of December 4, 2019, page 3, the auditee argues that the DPO previously in office "reported regularly to the Director Administrative and Financial in 2018” and that a particular context with regard to the recruitment of the current DPO has resulted in the latter "reporting to the Informal Administrative and Financial Director (…) until March 2019”. the

controlled then specifies that since March 15, 2019, the legal department and the DPD have been part of […], placed under the responsibility of the Chief Executive Officer and that since May 2019, a “formal activity report” is drawn up each month.

36. As for the content of the report drawn up by the DPO, the audit specifies on page 4 of its decision of position of December 4, 2019 that “The monthly activity report is (…) sent to the

Chief Executive Officer without the content of the report having been modified, unless supplemented by minutes of the meeting with the Administrative and Financial Director".

37. In its statement of December 4, 2019, the auditee also claims, on page 3, that "The report cites […] of Company A to raise a breach by making a partial quote: "the data protection officer reports directly to the highest level of the Company, namely the Board of Directors and the Executive management ". However, the CNPD omitted the part of the text of […] specifying that the DPO reports to the Board of Directors and to the General Management "for all significant problem arising or identified in the course of his duties".

38. The audit goes on to state that "The GDPR and the guidelines not specifying what should be the nature of the report made at the highest level of the hierarchy, Company A considered, in view of the size and organization of Company A, that it was preferable to discuss data protection issues at a lower level (heads of service which have the delegation of power to make decisions or even directors depending on the nature of the problem) in order to resolve them in the most efficient and to then report to the Director General. Of course, in the event that the DPO notices a significant blockage, he has the opportunity to contact the Management directly General and the Board of Directors. »

39. On this point, the Restricted Committee notes that the direct report at the highest level of the management is, according to […], conditioned on the existence of a "significant problem" (or "significant blocking", according to the position of the audited of December 4, 2019). Outraged the question of what are the criteria that make it possible to determine, in practice, the existence of such a problem, the Restricted Committee has reservations about this condition which could constitute an obstacle to the direct access of the DPO to the highest level of the management, in that the DPO could be in the position of having to justify the existence of such a "significant problem" before intervening with the highest level

of management. However, the Restricted Committee considers that the DPO should be able to circumvent the intermediate hierarchical levels as soon as he deems it necessary.

---

40. The Restricted Committee also notes in this respect that in its letter of 17 September 2020, the control informed the head of investigation of measures decided in this direction, namely that it will be added, in its "general policy for the management of personal data staff", the following indication: “the DPO, if he deems it necessary, can directly contact the Managing Director of Company A in order to report to him any problem ".

41. If measures have been decided during the investigation by the person inspected in the sense of brought into compliance, the Restricted Committee nevertheless agrees with the observation of the Chief of investigation according to which, at the beginning of the investigation, the controlled was not able to demonstrate that the DPO could act without receiving instructions with regard to the exercise of his duties or that he reported directly to the highest level of management.

42. The Restricted Committee finds that it does not have the documentation that would allow demonstrate that the measures described in point 40 of this Decision have been taken by the controlled.

43. In view of the foregoing, the Restricted Committee concludes that Article 38.3 of the GDPR has not been complied with by the controller.

C. On the breach relating to the mission of information and advice of the DPO

1. On the principles

44. Under section 39.1. a) of the GDPR, one of the tasks of the DPO is to “inform and advise the controller or processor and employees who

carry out the processing on the obligations incumbent on them under this

Regulation and other provisions of Union law or the law of the Member States in

matters of data protection".

2. In this case

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

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

"the organization has formal reporting of the activities of the DPO to the Committee of

Direction based on a defined frequency. With regard to information to employees, it is

expected that the organization has set up an adequate staff training system

on data protection".

46. On these two points, according to the statement of objections, page 4, "It appears from the investigation

that the personnel of Company A have been made aware by the DPO alone or accompanied by the

CISO. Specific training has been carried out for senior executives,

human resources and the IT department. With regard to the person responsible for

treatment, the DPO issues recommendations on an ad-hoc basis (13 between 25 May

2018 and February 4, 2019). In a logic of daily management of the protection of

data and given the volume of data processed, the sensitivity of some of

these data or the complexity of the processing operations (see remarks

preliminary), it is expected that the missions of information and advice with regard to the

controller are better formalized, for example with a report

of activity. It is then specified that during the investigation "the CNPD agents were

informed that there is now a monthly report for the Chief Executive Officer".

The Restricted Committee nevertheless notes that it does not have the documentation that would demonstrate that this measure has been put in place. This being specified, it is noted in the statement of objections, page 5, that at the start of the investigation, "the controller has not been able to demonstrate that the DPO exercises its information and advice missions with regard to the data controller. »

47. In its statement of December 4, 2019, the auditee first maintains “that neither the GDPR nor the guidelines impose any formalism regarding the way which the DPO performs its information and advisory tasks" and "that the absence of formal activity report on a regular basis is not sufficient to demonstrate that the DPO has not carried out its information and advisory missions. » The controlled person then describes how way the data protection officer carries out his missions of information and consulting “through, in particular, the review of contracts (provision of services, outsourcing, etc.), data protection impact assessments (DPIA) or more responses to requests from the various GDPR correspondents or services" and specifies that "the DPO is confronted every day with requests and issues related to data protection for which it issues an opinion either informal (telephone for example) or formal (most often email or report). »

48. With regard to the mission of informing employees of the obligations which they are incumbent under the GDPR, the controller indicates in its position paper of December 4

2021 that "[a]s pointed out by the CNPD, the DPD also carries out its missions information and advice during training and awareness sessions. »

49. In this regard, the Restricted Committee finds that the breach noted by the Chief

investigation only concerns the DPO's mission of information and advice with regard to
of the controller, and not the mission of information and advice of the DPO to
towards employees.

50. The Restricted Committee notes that Article 39.1 of the GDPR lists the missions that the
DPD must at least be entrusted with the mission of informing and advising the organization
as well as the employees, without however specifying whether specific measures must be
put in place to ensure that the DPO can fulfill his mission of information and
advice. The DPO Guidelines, which make recommendations and
best practices to guide data controllers in implementing
compliance with their governance, also only succinctly address the
advice and information mission of the DPO. Thus, they specify that keeping the register
processing activities referred to in Article 30 of the GDPR may be entrusted to the DPO and that
“[t]his register should be considered as one of the tools enabling the DPO to exercise its
missions to monitor compliance with the GDPR as well as to inform and advise the
controller or processor.8”

51. In the present case, the Restricted Committee notes that it appears from the investigation file that the DPO
been involved in the establishment of the register of processing activities and that it ensures a
followed by this register9.

52. The Restricted Committee further notes that in its position paper of 4 December
2019, the auditee provided elements to describe how the DPO carries out in
carries out its missions of information and advice with regard to the data controller.

53. Nevertheless, the Restricted Committee recalls that it has already noted in point 23 of the
this Decision that page 2 of the statement of objections rightly states
(under “preliminary remarks”) that “[t]he GDPR requirements 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

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

9 Visit report of February 4, 2019, p. 5

---

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

concerned. »

54. However, given that it has already been noted in point 24 of this Decision that

the activities of the controller involve the processing of personal data which

potentially affect a large number of people concerned, the training

restricted considers that formal reporting of the DPO's activities to management, on

the basis of a defined frequency, constitutes a proportionate measure in order to demonstrate

that the DPO carries out its missions of information and advice with regard to the person in charge of the

treatment.

55. The Restricted Committee notes that the audit indicated that formal reporting, on a

monthly basis, was set up during the investigation, but nevertheless agrees with the

finding of the head of investigation that, at the start of the investigation, the data controller

has not been able to demonstrate that the DPO carries out its missions of information and

advice to the data controller.

56. The Restricted Committee also points out that it does not have the documentation that

would make it possible to demonstrate that this measure was put in place by the controller.

57. In view of the foregoing, the Restricted Committee concludes that Article 39.1. a) of the GDPR has

not respected by the controller.

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

1. On the principles

58. According to section 39.1. b) of the GDPR, the DPO has, among other things, the mission of "monitoring compliance of this Regulation, other provisions of Union law or the law of the Member States 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 with regard to the distribution of responsibilities, awareness and training of staff involved in processing operations, and related audits reporting". Recital (97) clarifies that the DPO should help the organization to verify the internal compliance with the GDPR.

59. It follows from the DPO Guidelines10 that, in the context of its mission to control, the DPO may 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

60. It appears from the audit report that, for the head of investigation to consider objective 10 as completed by the auditee as part of this audit campaign, he expects that

“the organization has a formalized control plan for the protection of

data (even if not yet executed)".

61. According to the statement of objections, page 5, “It appears from the investigation that the organization

carries out checks on an ad hoc basis in the context of projects to which the DPO

participate. In a logic of daily management of data protection, and

given the volume of data processed, the sensitivity of some of this data

or the complexity of the processing operations (see preliminary remarks), it is

whereas the control missions of the DPO are better formalized, for example with

the establishment of a control plan. »

62. In its statement of December 4, 2019, the auditee argues "that it is not

because there is no formalized control plan that no adequate control of processing

data within the organization is carried out. Moreover, this control is often done

implicitly in the context of projects for which the DPO intervenes. Indeed, through

the review of the processing register, the DPIAs, the issues raised, the DPO

controls the application of the regulations and sends the information back to the hierarchy if necessary in order to

to regularize the situation. »

63. The Restricted Committee notes that Article 39.1 of the GDPR lists the tasks that the

DPD must at least be entrusted with the task of monitoring compliance with the GDPR, without

however, require the organization to put in place specific measures to ensure that

the DPO can carry out his control mission. Thus, the guidelines for

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

the DPOs specify 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 must be considered as one of the tools allowing the DPO to carry out its tasks of monitoring compliance of the GDPR as well as information and advice to the controller or sub-dealing.11”

64. The Restricted Committee has already noted in point 51 of this decision that it is apparent from the investigation file that the DPO was involved in establishing the register of activities of treatment and that it monitors this register12. The controlled, in his position of December 4, 2019, moreover argues that the DPO controls the application of the GDPR in particular “through the review of the processing register”.

65. Nevertheless, as has already been recalled in points 23 and 53 above, it is specified in rightly 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 the data controllers with regard to the sensitivity of the data processed and the risks incurred by the data subjects. »

66. However, given the fact that it has already been noted in point 24 of this Decision that the activities of the controller involve the processing of personal data which potentially affect a large number of people concerned, the training restricted considers that the control mission carried out by the DPO with the controlled should be further formalised, for example through a control plan for data protection, in order to be able to demonstrate that the DPO carries out its mission of adequate monitoring of GDPR compliance.

67. The Restricted Committee takes note of the fact that in its letter of 17 September 2020, the audited indicates that it has been decided "to put in place an audit and control strategy through the development in 2020 of a control plan". However, this decision being intervened during the investigation, the Restricted Committee agrees with the finding of the Chief

of investigation according to which the audited was not able to demonstrate that the DPO exercises its missions of monitoring compliance with the GDPR.

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

12 Visit report of February 4, 2019, p. 5

---

68. The Restricted Committee notes that it does not have the documentation that would allow to demonstrate that this measure has been put in place by the auditee.

69. In view of the foregoing, the Restricted Committee concludes that Article 39.1. b) of the GDPR has not respected by the controller.

III.

On the corrective measures and the fine

A. Principles

70. In accordance with article 12 of the law of 1 August 2018 organizing the National Commission for Data Protection and the General Data Protection Regime data protection, the National Commission has the powers provided for in Article 58.2 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. »

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

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

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

whether an administrative fine should be imposed and to decide on the amount of this

fine :

(a) the nature, gravity and duration of the breach, taking into account the nature, scope or

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

affected and the level of damage they suffered;

b) whether the breach was committed willfully or negligently;

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

damage suffered by the persons concerned;

d) the degree of responsibility of the controller or processor, 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".

72. The Restricted Committee wishes to specify that the facts taken into account in the context of the

this Decision are those found at the start of the investigation. The possible

subsequent changes relating to the subject of the investigation, even if they

allow full or partial establishment of conformity, do not allow

to retroactively cancel a violation found.

73. Nevertheless, the steps taken by the control to comply with the

the GDPR during the investigation procedure or to remedy the shortcomings identified

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

74. In his supplementary letter to the statement of objections of 10 August 2020, the head

of investigation proposes to the restricted formation to pronounce against the controlled a

administrative fine in the amount of 15,000 euros.

75. In his letter of September 17, 2020, the person inspected maintains "that the proposed sanction

to the Restricted Training is not consistent with the grievances invoked".

76. 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 by article 83.2 of the GDPR:

- As to the nature and gravity of the breach [Article 83.2 a) of the GDPR], with regard to breaches of Articles 38.1, 38.3, 39.1 a) and 39.1 b) 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, only in the event that the DPD is involved from the earliest possible stage in all questions relating to the data protection, exercises its functions and missions in complete independence, exercises its missions effectively, including the mission of informing and advising the manager processing and the task of monitoring compliance with the GDPR.
- As for the duration criterion [Article 83.2.a) of the GDPR], the Restricted Committee notes that the controlled indicated, in its letter of September 17, 2020:

(1) That it was decided to take measures in September 2020 in order to formalize involving the DPO in all matters relating to data protection. the breach of Article 38.1 of the GDPR therefore lasted over time, at least between May 25, 2018 and September 2020;

(2) That the DPO has been attached to […] since March 2019 and that it has been decided to take measures in September 2020 in order to formalize the possibility for the DPO, if he considers it necessary, to "contact the Chief Executive Officer directly in order to raise any problems with him". The breach of Article 38.3 of the GDPR therefore lasted at least between May 25, 2018 and September 2020.

(3) That it was decided to put in place “an audit and control strategy by

the development in 2020 of a control plan. » Breach of section 39.1. b) from

GDPR therefore lasted over time, at least between May 25, 2018 and September

2020.

With regard to the mission of information and advice, the restricted training falls under

that it appears from the audit report that the audit indicated that formal reporting was

implemented in May 2019. The breach of Article 39.1.a) of the GDPR therefore lasted for

at least between May 25, 2018 and May 2019.

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

Survey No. […] conducted with Company A

- 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 recalls the

findings made in point 24 of this Decision, namely that the audit counts

approximately […] employees (according to the investigation file), […].

- As to the degree of cooperation established with the supervisory authority [Article 83.2 f) of the GDPR],

the restricted formation takes into account the assertion of the head of investigation that the

auditee demonstrated constructive participation throughout the investigation.

- As to the categories of personal data affected by the breach

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

has an internal service […].

77. The Restricted Committee notes that the other criteria of Article 83.2 of the GDPR are not

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

administrative and its amount.

78. The Restricted Committee notes that while several measures have been decided by the controlled

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

decided only following the launch of the investigation by CNPD officials on

17 September 2018 (see also point 72 of this decision).

79. Consequently, the Restricted Committee considers that the imposition of an administrative fine

is justified with regard to the criteria set out in Article 83.2 of the GDPR for breach of the

Articles 38.1, 38.3, 39.1 a) and 39.1 b) of the GDPR.

80. 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 fixed for the violation the

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

of the GDPR is reproached to the controlled, the maximum amount of the fine that can be retained

amounts to 10 million euros or 2% of worldwide annual turnover, whichever is greater

high being retained.

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

restricted considers that the pronouncement of a fine of 15,000 euros appears both

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

---

2. Regarding the taking of corrective measures

82. 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 implementation of measures ensuring the formalized association and

documented from the DPO to all questions relating to data protection,

in accordance with the requirements of Article 38 paragraph 1 of the GDPR and the principle of

“accountability”. Although several ways can be envisaged to achieve
this result, one of the possibilities could be to analyze, together with the DPO, all the
relevant committees/working groups with regard to data protection and
formalize in writing the terms of his intervention (previous information of the agenda
meetings, invitation, frequency, permanent member status, etc.). It is to be remembered
that the DPO's presence on the various committees/working groups should enable him to be
directly and fully informed, but that this presence does not mean that the DPO has
necessarily a decision-making role.

b) Order the establishment and maintenance of a formal mechanism guaranteeing
the autonomy of the DPO in accordance with the requirements of Article 38 paragraph 3 of the GDPR.
Several ways can be considered to achieve this result, such as
attach the DPO to the highest level of management in order to guarantee his
autonomy or to create a formalized and regular line of direct reporting, as well as a
formal emergency escalation mechanism to management to circumvent the
intermediate hierarchical level(s) on the initiative of the DPO.

c) Order the formal and documented deployment of the DPO monitoring mission
in accordance with Article 39 paragraph 1 b) of the GDPR and the principle of "accountability".
Although several ways can be implemented to achieve this result, the
DPD should document its checks on the application of internal rules and procedures
in terms of data protection (second line of defence). This documentation
could take the form of a control plan followed by control and audit reports. »

83. As to the corrective measures proposed by the head of investigation and with reference to point
73 of this decision, the Restricted Committee takes into account the steps
carried out by the controlled in order to comply with the provisions of Articles 38.1, 38.3, and
39.1 b) of the GDPR, as detailed in its letter of September 17, 2020. More
in particular, it takes note of the following facts:

- With regard to the violation of Article 38.1 of the GDPR, measures have been decided by the control in order to ensure the association of the DPO to all the questions relating to data protection. Indeed, the audit decided to "formalise monthly meetings between the DPO and the heads of departments that process the most data personal […] (…) as well as biannual meetings with the other heads of services" and to add "as an appendix to the general data management policy, a sheet allowing each person in charge of a project to deal with the DPO data protection issues". Nevertheless, the restricted formation does not have no documentation demonstrating that such compliance measures have been taken in compliance by the control. The Restricted Committee therefore considers that there is to pronounce the corrective measure proposed by the head of investigation under a).
- With regard to the violation of Article 38.3 of the GDPR, the controller recalls that the DPD has been attached to […] since March 2019 and indicates that the following indication will be added in the general personal data management policy of the Company A: "the DPO, if he deems it necessary, can directly contact the Managing Director of Company A in order to report any problems to him » The Restricted Committee considers that such a measure would allow the DPO, if he considers necessary, circumvent the intermediate hierarchical levels. Nevertheless, the restricted training does not have the documentation to demonstrate that this compliance measure was taken by the auditee. Restricted training therefore considers that it is appropriate to pronounce the corrective measure proposed by the head of investigation under b).

- With regard to the violation of Article 39.1 b) of the GDPR, the audited states that it
was decided "to put in place an audit and control strategy by drawing up
in 2020 of a control plan". Nevertheless, the restricted formation does not have
documentation to demonstrate the implementation of this compliance measure
in compliance by the control. The Restricted Committee therefore considers that there is
to pronounce the corrective measure proposed by the head of investigation under c).
84. With regard to the violation of Article 39.1 a) of the GDPR, taking into account the findings
made in points 55 and 56 of this decision, the Restricted Committee considers that there
instead of ordering the implementation of corrective measures to ensure that the DPO

---

exercises, in a formal and documented way, its mission of information and advice with regard to
of the controller.
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, 38.3, 39.1 a) and 39.1 b) of the GDPR;
- to impose an administrative fine on Company A in the amount of fifteen
one thousand euros (15,000 euros) with regard to the violation of articles 38.1, 38.3, 39.1 a) and 39.1 b)
GDPR;
- to pronounce against Company A, an injunction to comply with the
Article 38.1 of the GDPR, within four months of notification of the decision to
restricted training, the supporting documents for compliance must be sent to the
restricted training at the latest within this period, in particular:
ensure the formalized and documented association of the DPO with all matters relating to

data protection;

- to pronounce against Company A, an injunction to comply with the

Article 38.3 of the GDPR, within four months of notification of the decision to

restricted training, the supporting documents for compliance must be sent to the

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

ensure the establishment and maintenance of a formal mechanism guaranteeing the autonomy

the DPO;

- to pronounce against Company A, an injunction to comply with the

Article 39.1 b) of the GDPR, within four months of notification of the decision

of the restricted training, the proof of compliance must be sent to the

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

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

- to pronounce against Company A, an injunction to comply with the

Article 39.1 a) of the GDPR, within four months of notification of the decision

of the restricted training, the proof of compliance must be sent to the

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

ensure that the DPO exercises, in a formal and documented manner, his mission of information and

advice to the controller.

Thus decided in Belvaux on June 11, 2021.

For the National Commission for Data Protection sitting in restricted formation

Tine A. Larsen Thierry Lallemang

President

Commissioner

Marc Lemmer

Commissioner

Indication of remedies

This administrative decision may be subject to an appeal for review within three

months following its notification. This appeal is to be brought before the administrative court and must

must be introduced through a lawyer at the Court of one of the Bar Associations.

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

Survey No. […] conducted with Company A