Decision of the National Commission sitting in restricted formation on

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

Deliberation No. 42FR/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. 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

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

1/13

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 Commission for Data Protection (hereinafter: the “Commission Nationale” 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 than 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 […], L-[…] and registered in the trade and companies register Luxembourg 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 controlled [is active in retail trade in non-specialized stores in food predominance].

4. By letter dated September 17, 2018, the head of investigation sent a questionnaire preliminary to the control to which the latter replied by email of October 8, 2018. A on-site visit took place on 27 February 2019 and a telephone meeting took place on 22 February 2021.

5. As part of this audit campaign, in order to verify the organization's compliance with Section 4 of Chapter 4 of the GDPR, the head of investigation has defined eleven control objectives included in the report of the visit of February 27, 2019, namely:

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

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

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

4) Ensure that the DPO has sufficient expertise and skills to

carry out its missions effectively;

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

6) Ensure that the DPO has sufficient resources to 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 15 March 2021 (hereinafter: the "statement of objections"), the head

of investigation informed the control of the breaches of the obligations provided for by the GDPR

that he noted during his investigation as well as the corrective measures and sanctions that he

proposes to the National Commission sitting in restricted formation (hereafter: the

“restricted formation”) to adopt.

7. In particular, the head of investigation noted in the statement of objections a

breach of the obligation to appoint a DPO2 and proposed to the Restricted Committee

to adopt a corrective measure as well as to impose an administrative fine of one

amount of 80,000 euros.

8. By letter dated April 12, 2021, the inspector sent his observations to the head of investigation

regarding the statement of objections.

9. By letter dated June 2, 2021, the President of the CNPD informed the controller of the date of

the session during which the case concerning him was registered and of the option

was offered to be heard there. By letter dated June 29, 2021, the controller informed the

President of the CNPD that he would not attend.

10. The case was on the agenda of the Restricted Committee meeting of July 14, 2021.

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

National, the Chief Investigator made oral submissions on the case and responded

to the questions posed by the Restricted Committee.

2 Objective #1

II.

Place

A. On the failure to appoint a DPO

1. On the principles

11. According to Article 37.1 of the GDPR, “The controller and the processor designate

in any case a data protection officer when:

(a) the processing is carried out by a public authority or a public body,

the exception of courts acting in the exercise of their judicial function;

(b) the core activities of the controller or processor consist of

processing operations which, due to their nature, their scope and/or their

purposes, require regular and systematic monitoring on a large scale of people

concerned; Where

(c) the core activities of the controller or processor consist of

large-scale processing of special categories of data referred to in Article

9 and personal data relating to criminal convictions and

offenses referred to in Article 10.

12. The Article 29 Data Protection Working Party adopted on 13 December

2016 DPO Guidelines which have been taken over and re-approved by

the European Data Protection Board dated 25 May 20183. These lines

guidelines provide clarifications concerning the notions of “basic activities” and

“large scale” which are found in article 37.1.b) and c) of the GDPR as well as concerning

the notion of “regular and systematic monitoring” found in Article 37.1.b) of the GDPR.

13. With regard to the notion of “core activities”, the guidelines specify that

“[t]he “basic activities” can be considered as the essential operations

to achieve the purposes of the controller or processor. They

also include all activities for which the processing of data is

an integral part of the activity of the controller or processor”.

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

4 WP 243 v.01, version revised and adopted on April 5, 2017, p. 24

---

14. With regard to the notion of “large scale”, it is recommended in the guidelines for

consider the following factors:

“- the number of persons concerned, either in absolute value or in relative value by

relation to the population concerned;

- the volume of data and/or the spectrum of data processed;

- the duration, or permanence, of the data processing activities;

- the geographic scope of the processing activity”5.

15. Finally, with regard to the notion of “regular and systematic monitoring”, the lines

guidelines clarify that tracking is not limited to the “online environment” 6. The term

“regular”, according to the guidelines, covers “one or more of the meanings

following:

- continuous or occurring at regular intervals over a period of time;

- recurring or repeating at fixed times;

- taking place constantly or periodically. »

As for the term "systematic", it covers "one or more of the meanings

following:

- occurring in accordance with a system;

- prearranged, organized or methodical;

- taking place as part of a general program of data collection;

- carried out within the framework of a strategy. » 7

2. In this case

16. As part of this audit campaign, for the head of investigation to consider the objective

1 as completed by the auditee, he expects the organization to have appointed a DPO on the 25

May 2018 if its processing falls within the scope of Article 37.1 of the GDPR.

17. It should be noted that the auditee carried out a documented analysis, as is

recommended by the DPD guidelines8, by which it arrived at the

conclusion that he was under no obligation to appoint a DPO. This analysis was

5 WP 243 v.01, version revised and adopted on April 5, 2017, p.25

6 WP 243 v.01, version revised and adopted on April 5, 2017, p.25

7 WP 243 v.01, version revised and adopted on April 5, 2017, p.26

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

---

transmitted by the control with its answers to the preliminary questionnaire by e-mail from the

October 8, 2018.

18. It emerges in particular from this analysis that the auditee “considers that if [his] activities

may sometimes include a dimension of large scale or regular monitoring […] [its]

activities do not involve the two elements together. "It is also stated that

the controlled “does not carry out regular monitoring for customer activities (no profiling). The

purchases are sometimes recorded on the customer card (at the will of the customer) but are not

used for direct marketing purposes. These data are processed solely for the purposes

restocking, customer relations when the latter calls or for the calculation of his points and

to fulfill legal obligations. »

19. In the Statement of Objections, the Head of Investigation refers to this analysis on page 5, “[i]t

The investigation shows that [the auditee] did not appoint a DPO. CNPD officials

take due note that, in accordance with the Group's DPO guidelines

"article 29" working paper on data protection [the auditee] has documented an analysis

internally in collaboration with its consultants (…) in order to determine whether or not there is

instead of appointing a DPO. Based on this internal analysis, the position [of the controlled] is

that a DPO does not seem necessary with regard to the activities carried out. »

20. The head of the investigation then notes that the person checked “offers a loyalty card service to its customers and that there are more […] active customer cards (i.e. used in the year). As part of the management of these customer cards, [the auditee] carries out data processing including purchase history and loyalty points. The cards loyalty schemes (…) operate in all the stores [of the controlled], as well as in other partner stores. “According to the head of the investigation, “the proposal of a loyalty program is an integral part of the activity [of the controlled]”; it would be by consequence of a "basic activity" of the control taking into account the clarifications provided in the DPO Guidelines on this notion9.

21. As to the question of whether the auditee carries out systematic and regular follow-up on database collected via the loyalty card, the head of the investigation considers that “[i]t The elements of the survey show that the [loyalty] card makes it possible to track purchases of a person through loyalty points. Follow-up is organized, occurs in accordance

9 WP 243 v.01, version revised and adopted on April 5, 2017, p. 24

to a system ([…]) and is carried out within the framework of a strategy, here a strategy of loyalty. The argument that the cardholder uses it "at will" is inoperative. Indeed, (…) the loyalty program is part of a strategy that encourages the cardholder to use it to earn points. As soon as a customer enters the loyalty program, it enters into a systematic and regular monitoring system. Although the purpose of "monitoring" may not be pursued as such by the person responsible for processing, the fact remains that to achieve the purposes pursued (restocking,

customer relationship, etc.), the data controller has set up a monitoring system

systematic and regular. »

22. With regard to the notion of “large scale”, the head of investigation first notes “that it

there are more than […] active [loyalty] cards” […]. Then, with regard to the extent

geographic, he notes that said card "can be used in all the stores [of the

controlled] in the country as well as in many other partner brands. " Finally,

concerning the duration of the processing, the head of the investigation notes that the loyalty card

allows “to trace the purchases of its holder over a period of two years”. Leader

investigation concludes that “[g]iven the number of people involved, the

the geographical extent of the processing activity, as well as its duration (…) the map [of

fidelity] must (…) be considered as large-scale processing within the meaning of Article

37 paragraph (1) GDPR. »

23. Taking into account the criteria examined by the head of investigation in order to determine whether the control

was and remains under the obligation to appoint a DPO, the Restricted Committee concludes that this

are those of Article 37.1.b) of the GDPR, which is however not explicitly mentioned

in the statement of objections, which refers only to Article 37.1 of the

GDPR. The Restricted Committee also notes that it is essentially on the basis of

the analysis of the “management of customer cards” (or “[loyalty] card”) processing that the head

of investigation came to the conclusion that the controlled was and remains under the obligation to

designate a DPO under Article 37.1.b) of the GDPR.

24. In its position paper of April 12, 2021, the auditee also returns in particular to

the processing in question and maintains that it does not constitute systematic monitoring,

considering that “the recording of data may possibly be considered

as systematic (after each purchase and presentation of the card) but in no case

the follow-up. The purpose of card processing is not to track purchases or

---

behaviors of its customers. (…) a mere registration cannot be considered
as a follow-up. »

25. The controlled further argues that the processing is not regular, considering that the
“customer card management” processing does not fall under any of the meanings of the term
"regular" retained by the guidelines for DPD10.

26. The auditee also indicates that the identification of the user of the loyalty card is not
not necessary to use it and that “[i]t is not uncommon for people to share
their card making any follow-up, which is not the case here, inoperative and ineffective. »

27. As mentioned in point 23 of this decision, it is essentially on the basis of
the basis of the analysis of the “management of customer cards” (or “[loyalty] card”) processing
that the head of investigation has come to the conclusion that the controlled person was and remains in
the obligation to designate a DPO under Article 37.1.b) of the GDPR. There is therefore place
to examine whether the processing in question covers each of the criteria set out in Article
37.1.b) GDPR.

28. As to the question whether the “management of customer cards” (or “[loyalty] card”)
constitutes a basic activity of the controller, given the fact that the
DPO guidelines specify that core activities “include
(…) all activities for which data processing is an integral part of
the activity of the data controller”11, the restricted training concurs with the assessment
of the head of the survey according to which "the proposal for a loyalty program is part of
integral to the activity [of the controlled]” and therefore constitutes a basic activity of
this last.

29. As to the notion of “large scale”, in the light of the recommendations made

in the DPO Guidelines on this notion12, and in particular

taking into account the fact that the number of persons concerned "in relative value by

relation to the population concerned", that "the geographical extent of the activity of

treatment" and that the duration of treatment are factors that should be considered

10 WP 243 v.01, version revised and adopted on April 5, 2017, p.26

11 WP 243 v.01, version revised and adopted on April 5, 2017, p.24

12 WP 243 v.01, version revised and adopted on April 5, 2017, p.25

---

into consideration, the Restricted Committee concurs with the assessment of the Head of Investigation according to

which "the [loyalty] card must (…) be considered as a high-level treatment

scale within the meaning of Article 37 paragraph (1) of the GDPR. »

30. Finally, it should be examined whether the "customer card management" (or "customer card"

fidelity]") constitutes a "regular and systematic monitoring" of the persons concerned.

31. The Restricted Committee admits that the "customer card management" (or "customer card"

[of loyalty]") is carried out "in accordance with a system". It nevertheless notes,

taking into account in particular the details provided by the auditee in its statement of 12

April 2021, referenced in points 24, 25 and 26 of this Decision concerning the

different aspects of this processing, that it does not appear from the investigation file that the said

the purpose of the processing would be regular monitoring of the data subjects or that such monitoring

would actually be carried out by the controller.

32. Therefore, it should be noted that it does not appear from the investigation file that the controlled

is found, due to the "management of customer cards" (or "[loyalty] card") processing,

under the obligation to appoint a DPO under Article 37.1.b) of the GDPR.

33. In view of the foregoing, the Restricted Committee concludes that the breach of Article 37.1 of the GDPR is not constituted.

III.

On the corrective measures and the fine

A. Principles

34. In accordance with article 12 of the law of 1 August 2018 on the organization of 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. »

35. 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 object, 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”.

B. In the instant case

1. Regarding the imposition of an administrative fine

36. In the statement of objections of 15 March 2021, the head of investigation proposes to the restricted committee to pronounce an administrative fine against the auditee relating to the amount of 80,000 euros “for breach of obligations arising from the GDPR in relation to the appointment of the Data Protection Officer”.

37. Since the breach of Article 37.1 of the GDPR has not been established, there is no need to pronounce against the audited the administrative fine proposed by the head of the investigation.

2. Regarding the taking of corrective measures

38. In the statement of objections of 15 March 2021, the head of investigation proposes to the Restricted Panel to take the following corrective action, specifying that it should be implemented "within 6 months, under penalty of a penalty payment of 1,000.- Euros per day of delay”:

“Order the controller to appoint a Data Protection Officer in accordance with Article 37, paragraphs (1) of the GDPR. »

39. Since the breach of Article 37.1 of the GDPR has not been established, there is no need to examine the related corrective action.

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

- to close the investigation opened by deliberation n°[…] of September 14, 2018 of the National Data Protection Commission at Company A located […], L-[…] and registered in the Luxembourg Trade and Companies Register under number[…], in

the absence of breach found against him.

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.
