Decision of the National Commission sitting in restricted formation on

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

Deliberation no. 22FR/2022 of December 13, 2022

The National Commission for Data Protection sitting in restricted formation,

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

Herrmann, commissioners;

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

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

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

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

data and the general data protection regime, in particular its article 41;

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

adopted by decision no. 3AD/2020 dated January 22, 2020, in particular its article 10.2;

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

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

its article 9;

Considering the following:

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

Survey no. […] conducted with Company A.

I. Facts and procedure

1. During its deliberation session of 17 July 2020, the National Commission sitting in

plenary formation (hereafter: the “Plenary Formation”) has decided to open an investigation

with Company A on the basis of article 37 of the law of August 1, 2018 on the organization

of the National Commission for Data Protection and the general regime on the

data protection (hereinafter: the “Law of 1 August 2018”) and to designate Mr.

Christophe Buschmann as head of investigation.

The said decision specified that the investigation carried out by the National Commission for the

data protection (hereinafter: the “CNPD” or the “National Commission”) had

for the purpose of monitoring the application and compliance with the GDPR and the law of August 1, 2018, and

specifically compliance with Articles 12.1, 13 and 14 of the GDPR.

2. Company A is […] registered with the Trade and Companies Register of Luxembourg

under number […], with registered office at L - […], […] (hereinafter: the “controlled”).

The controlled [is active in the operation of internet portals and the provision of services via these

portals].

3. The decision of the National Commission sitting in restricted formation (hereafter: the

“Restricted Training”) on the outcome of the investigation will be based:

~

on the processing carried out by the controller in relation to the operation of the site

website [of Company A] (hereinafter: the “website”) and controlled by the agents of

the CNPD; And

~

on the legal and regulatory provisions taken into account by the head of investigation

in its statement of objections.

The auditee clarified that he does not operate a mobile application.1

4. By letter dated August 26, 2020, the head of investigation sent a preliminary questionnaire.

This moment is later referred to in this decision as "at the beginning of

investigation ". The control responded by email of September 22, 2020. After a visit to

1 See page 7 of the completed preliminary questionnaire.

Survey no. […] conducted with Company A.

place which took place on October 9, 2020, the control and the CNPD investigation service carried out an exchange of letters.2

5. Following this exchange, the head of investigation drew up Investigation Report No. […] based on the deliberation of July 17, 2020 relating to compliance with Articles 12 point 1, 13 and 14 of the GDPR dated April 29, 2021 (hereinafter: the “Investigation Report”).

It appears from the investigation report3 that in order to structure the investigation work, the chief investigation has defined nine control objectives, namely:

1) Make sure the information is available;

2) Ensure that the information is complete;

3) Ensure that the absence of information is motivated by a valid exception;

4) Ensure that information is transmitted by appropriate means;

5) Ensure that information is concise, transparent, understandable, and conveyed in clear and simple terms;

6) Ensure that the information is adapted to the category of persons concerned;

7) Ensure that information is free;

8) Ensure that information is easily accessible; And

9) Ensure that the information is transmitted during the key stages of the processing.

It is specified in the investigation report that the CNPD agents did not check “the legality of the processing carried out by the controller”. In this context, it is given the following example: “in the event that the controller informs the persons concerned that their personal data are kept for a period 2 years, CNPD officials will be able to check that the controller does not not retain said data for a different period. On the other hand, the agents of the

2 See Statement of Objections, point 9 for a detailed list of exchanges throughout the investigation.

3 Investigation report, page 7, point “3.1 Control objectives”.

CNPD will not comment on the legality of this 2-year period applied by the
controller. »4

The survey also focused on users of the website and did not target
other categories of data subjects such as employees of the audited.5 The
users are in this case the customers […] “of Company A” and more specifically […].6

The investigation report is annexed to the documents collected by the investigation department of the
CNPD and on which the investigation report is based (appendix 1), as well as the
report of the on-site visit by CNPD agents of October 9, 2020 mentioned above (appendix 2)
(hereinafter: the “Report”).

6. During its deliberation session of July 23, 2021, the Plenary Formation appointed
Mr. Marc Lemmer, commissioner, as head of investigation replacing
Mr. Christophe Buschmann, resigned.

7. At the end of his investigation, the head of investigation notified the person inspected on
13 January 2022 a Statement of Objections (hereinafter: “Statement of Objections”)
detailing the shortcomings that he considered constituted in this case in relation to the requirements
prescribed by Articles 12.1 (obligation of transparency) and 13 of the GDPR (right to
information).

The head of investigation proposed to the Restricted Panel to adopt seven corrective measures
different, as well as to impose on the controlled an administrative fine of an amount of
1,700 euro.

8. The audited responded to the statement of objections by letter dated February 10, 2022.

9. By letter dated May 20, 2022, the president of the Restricted Formation informed the controlled that his case would be registered for the Restricted Panel session of July 13, 2022 and that he could attend this meeting. The controller has confirmed his presence at the said meeting dated June 21, 2022.

10. During this session the head of investigation, Mr. Marc Lemmer, was present. Control was represented by […]. The head of the investigation and the representative of the control presented their oral submissions in support of their written submissions and responded to questions

4 Investigation report, page 7, point “2.3 Reservations”.

5 Investigation report, page 6, point “2.2 Scope”.

6 Investigation report, page 9, point “4.2 Description of the inspection”.

posed by the Restricted Panel. The Restricted Formation gave the controlled the possibility of sending additional information requested within one week during that session. The controller spoke last.

11. By email of July 13, 2022, the auditee sent the additional information requested by the Restricted Formation on the same day.

II. Place

II. 1. On the reasons for the decision

A. On the breach related to the obligation of transparency

1. On the principles

12. According to Article 12.1 of the GDPR, the “controller shall take measures appropriate to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and Article 34 with regard to

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

understandable easily accessible, in clear and simple terms, in particular for

any information intended specifically for a child. The information is provided by

in writing or by other means including, where appropriate, electronically.

When the data subject so requests, the information may be provided

orally, provided that the identity of the data subject is demonstrated by other

means. »

13. Transparency is a fundamental aspect of the principles relating to the treatment of

personal data.7 The obligations in this area have been clarified by the

Article 29 Working Party in its guidelines on transparency within the meaning of the

Regulation (EU) 2016/679, the revised version of which was adopted on April 11, 2018 (hereinafter:

“WP 260 rev.01” or the “transparency guidelines”).

These guidelines explain in particular the general rules of transparency

established by Article 12 of the GDPR, and which are applicable to the communication of information

to data subjects (Articles 13 and 14 of the GDPR), to communications addressed

to data subjects regarding the exercise of their rights (Articles 15 to 22 of the

7 See in particular Articles 5.1.a) and 12 of the GDPR, see also recitals (39), (58) to (60) of the GDPR.

GDPR), and communications regarding data breaches (Article 34 of the

GDPR).8

They also underline that a “primary aspect of the principle of transparency put in place

light in these provisions is that the data subject should be able to

determine in advance what the scope and consequences of the processing encompass in order to

not to be caught off guard at a later stage as to how their data

of a personal nature were used. »9

14. It should be noted that the European Data Protection Board (hereinafter: the “EDPS”), which

succeeded the Article 29 Working Party on 25 May 2018, took over and reapproved the

documents adopted by the said Group between May 25, 2016 and May 25, 2018, as

specifically the aforementioned guidelines on transparency.10

2. In this case

2.1. Regarding the requirement to provide information in a “concise and transparent” way

15. In the context of objective 211 the head of investigation expected, among other things, that “the

following information is accessible through the data protection policy,

in accordance with the appendix to the guidance of the Article 29 Working Party on

information to be communicated to a data subject under Article 13

or Article 14 of the GDPR:

[…] - The contact details of the DPO (if appointed) (cf. Test 2), […]

- The data retention period or, when this is not possible, the criteria

used to determine this period (cf. Tests 8 and 21), […]. »

CNPD officers therefore inspected Company A's privacy policy.

available on the website of the controller and whose last update at the time of

the analysis by CNPD officials dated from […] 201812 (hereinafter: the “policy of

confidentiality”) and noted that it indicated that the auditee had appointed a

8 WP 260 rev.01, point 7.

9 WP 260 rev.01, point 10.

10 See

https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

11 “Objective 2 - Ensure that the information is complete”; Investigation report, page 15 et seq.

12 See Exhibit 1 appended to the investigation report.

Endorsement decision

of the EDPS

May 25

1/2018

2018,

of

available

below :

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

Survey no. […] conducted with Company A.

6/35

Data Protection Officer (hereinafter: "DPD"). On the other hand, “it turns out, after

interview of CNPD officials with the manager of Company A, that this information

are wrong. Indeed, Company A has not appointed a DPO (see Test 2) […]. »13

In addition, CNPD officials compared “the length of detention indicated in the

data protection policy (or, if applicable, the details available

in the processing register) with the system configuration respectively the data

oldest available. […] Regarding one of the cookies, it was found that the duration of

retention was 2 years i.e. much higher than that indicated in the protection policy

data and this with or without user acceptance (Exhibit 16, […]).”14

16. In the context of objective 515 the head of investigation expected, among other things, that “the

data protection policy reflects the reality of the processing actually carried out

place, that is to say without anticipation of processing that could possibly be put

in place by the controlled in the future (cf. Test 5)”.

In this context, CNPD officials “inspected the data protection policy

data to verify that it reflects the reality of the processing operations actually implemented,

that is to say without anticipation of processing that could possibly be implemented

place by the controlled in the future. To do this, CNPD officials compared the

content of the data protection policy with the explanations obtained from the

checked during the interview on 09/10/2020. 16 They realized during this

inspection that a processing indicated in the privacy policy was in fact not

carried out, in this case profiling. Following the interviews conducted with the controller in

dated October 9, 2020, CNPD officials noted that such processing was not in effect.

reality not realized, but mentioned in the data protection policy for

anticipate the integration of future activities. However, it appears from the investigation report that “it is

given that the data protection policy reflects the reality of the processing

actually put in place, i.e. without anticipating processing that could

possibly be put in place by the controller in the future. »17

13 Investigation report, page 28, point “4.4.2.3.1 Inaccuracy of information”.

14 Investigation report, page 28, point “4.4.2.2.20 Test 21: Verification of the length of detention”.

15 “Objective 5 - Ensure that information is concise, transparent, understandable, and transmitted in

clear and simple terms”; Investigation report, page 35 et seq.

16 Investigation report, page 38, point “4.4.5.2.5 Test 5: Implementation vs. Anticipation”.

17 Investigation report, page 38, point “4.4.5.2.5 Test 5: Implementation vs. Anticipation. »

17. In addition, the “CNPD agents inspected the website and the policy of

company A’s data protection to assess the conciseness and transparency of the

information provided, as well as the effectiveness and succinct nature of their

presentation. »18

In this context, they noted with regard to retention periods "a

inconsistency between the retention period indicated in the data protection policy

data (6 months after the last use of personal data) and that of the register

processing (until the account is closed). »19

18. In the Statement of Objections, the Head of Investigation therefore noted that certain

information contained in the data protection policy of the controlled does not

did not reflect reality, because the policy referred to the use of the technique of

profiling not put in place by the controlled and it indicated that the controlled had appointed a

DPD, whereas this was not the case at the time of the CNPD's visit.20

In addition, the head of investigation referred to the two cases “for which there is a

difference between the retention period indicated in the privacy policy and the

retention period actually applied.

The first case concerns the cookies policy which indicates that without action on the part of

the user, cookies have a lifespan limited to a maximum of 13 months, this duration

not being extended automatically during new visits to the site. The agents

of the CNPD however found that the retention period of one of the cookies ([…]) was

actually 2 years, contrary to what is indicated in the policy.

The second case concerns the data protection policy which mentions a duration

retention period of 6 months after the user's last connection to the site, while in

In reality, customer order data is deleted after closure

of the user's account, as indicated in the processing register. »21

Thus, the head of the investigation held that "the conditions of article 12.1 of the GDPR with regard to the

fairness and transparency of information have not been respected”.22

18 Investigation report, page 36, point “4.4.5.2.1 Test 1: Concise and transparent”.

19 Investigation report, page 36, point “4.4.5.2.1 Test 1: Concise and transparent”.

20 Statement of Objections, point 18.

21 Statement of Objections, point 18.

22 Statement of Objections, paragraph 20.

---

19. The Restricted Committee recalls that Article 12.1 of the GDPR requires, among other things, that required information is provided in a concise and transparent manner.

She notes that the Transparency Guidelines state that “the requirement that the provision of information to data subjects and that communications to them are addressed are carried out in a “concise and transparent” manner means that the controllers should present the information/communications in a way effective and succinct in order to avoid overwhelming the persons concerned with information. »23

20. The Restricted Committee notes that the confidentiality policy mentioned in the part […] the following: “[…] This processing involves a profiling technique. »24

However, even if it was stated in the privacy policy, it appears from the Account-Rendering that the controlled did not perform behavioral analyses, i.e. at the profiling and that “this discrepancy was due to the fact that at the time of writing the data protection policy, Company A did not yet know precisely its scope of action. »25

21. It also notes that the confidentiality policy mentioned that the controlled had appointed a DPO, although he had specified during the on-site visit of October 9, 2020 “that he Strictly speaking, there was no “official” DPD. According to articles 37 to 39 of the GDPR and the agency's internal analysis, Company A concluded that the appointment of a DPD was not required.”26

22. The Restricted Training therefore considers that the provision of information to users

which correspond to processing which is not carried out, i.e. profiling, or

which do not reflect reality, so the erroneous mention of the appointment of a DPO, was sowing

confusion and prevented the required information from being presented to

website users efficiently and succinctly.

23. She further notes that the guidelines on transparency indicate that a

“primary aspect of the principle of transparency highlighted in these provisions is

that the data subject should be able to determine in advance what the

scope and consequences of the processing encompass so as not to be caught unawares

23 WP 260 rev.01, point 8.

24 See page 2 of the privacy policy.

25 Minutes of October 9, 2020, page 9.

26 Minutes of October 9, 2020, page 8.

---

at a later stage as to how his personal data has been

used. 27 It follows that the data controller must provide data subjects

concerned accurate and complete information on all processing

performed on their personal data.

24. The Restricted Committee notes in this respect that there is a difference between the duration of

retention indicated in the privacy policy for personal data

user’s personnel (“six months from the last connection to the Site”) and the

retention period mentioned in the register of processing activities of the controller (here

after: the “register”).28 Indeed, according to the register, the deletion of data29 only takes place

only after the closing of the client's account, except for the accounting data which is

saved for 10 years.30 As a result, the auditee did not provide any information

accurate on all processing carried out on personal data

users, and more specifically on the retention period of personal data

user staff.

25. In view of the foregoing, the Restricted Panel therefore agrees with the opinion of Chief

investigation that at the start of the CNPD31 investigation there was a breach of the obligation

transparency resulting from Article 12.1 of the GDPR and with regard to Article 13.1.b) and

13.2.a) of the GDPR, and more specifically the requirement to provide the required information

in a concise and transparent manner.

26. As for the measures taken by control after the on-site visit by CNPD agents,

the Restricted Panel comes back to this in point 64, as well as in Chapter II.2, Section 2.2 of this

decision.

27. Finally, with regard to the retention period of one of the cookies ("[...]"), the

Restricted Training reminds that the filing or reading of information on the equipment

user terminal are governed by the amended law of 30 May 2005 relating to

specific provisions for the protection of the person with regard to the processing of data

of a personal nature in the electronic communications sector (hereinafter: “Law

amended on May 30, 2005”). If the use of cookies leads in addition to said deposit or

reading information on the user's terminal equipment "on collection (or at any

27 WP 260 rev.01, point 10.

28 See Exhibit 9 attached to the investigation report.

29 This concerns the following data: Surname, First name, Address, Password (if creating an account).

30 This concerns the following data: Accounting/administrative data […].

31 Statement of Objections, point 20.

other processing) of personal data (for example, when cookies are
used to collect data on a user's shopping preferences
determined), all the rules of the GDPR will also have to be respected, which implies
in particular that the processing must be based on a distinct condition of lawfulness (Article 6
of the GDPR) and that information in accordance with Articles 12 to 14 of the GDPR must be provided
to the data subject".32

Indeed, the case law of the Court of Justice of the European Union33 has confirmed that it is
possible that the processing falls both within the material scope of the Directive
"privacy and electronic communications"34 and that of the GDPR.35

However, as the control of the application and compliance with the aforementioned law of 30 May
2005 was not within the scope of the investigation in question, the Restricted Panel does not rule
not in this decision on the compliance of the audit with the requirements
posed by this law.

2.2. As to the requirement to provide information in an "easily accessible" way

28. In the context of objective 436 the head of investigation expected, among other things, that
"that all substantial updates to the data protection policy
are the subject of active communication (informative e-mail, pop-up on the website,
etc.) with a summary of the (main) modifications (cf. Test 5). »37

CNPD officials noted that "it was clarified during the interviews conducted
that in the event of a change in the data protection policy, Company A would inform
users by email, which is in contradiction with the indications of the policy of
data protection which specifies that it is the responsibility of users to

32 CNPD guidelines on cookies and other tracers, point 2., available at:

https://cnpd.public.lu/fr/dossiers-thematiques/cookies/legal-context.html.

33 “Planet 49” case, CJEU, C-673/17, 1 October 2019, points 42 and 65.

34 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector,

as amended.

35 EDPS, Opinion 5/2019 on the interactions between the “Privacy and Electronic Communications” Directive and the GDPR, in particular with regard to the competence, tasks and powers of data protection authorities

of data, adopted on March 12, 2019, point 30. et seq.

36 “Objective 4 - Ensure that information is transmitted by appropriate means; Investigation report,

page 32 et seq.

37 Investigation report, page 31, Ad Objective 4, point “4.4.4.1 Expectations”.

---

find out about any changes to the data protection policy (cf.

Testing 5). »38

29. For this reason, the head of the investigation held that the "conditions of article 12,

paragraph 1 of the GDPR regarding the accessibility of information (at the level of updates)

have not been respected. »39

30. Restricted Training refers in this context to the guidelines on the

transparency indicating that the "readily accessible" criterion means that the person

concerned should not have to search for the information but should be able to

access it […]” and that the “controller should respect the same

principles when communicating the initial opinion or declaration on the protection of life

privacy and any subsequent material changes to this notice or this

declaration” and “that a change notification should always be communicated

by a suitable means (for example, e-mail, postal mail, pop-up window on a

web page or other means that effectively captures the attention of the data subject)

specifically devoted to modification (for example, separate from a content of

direct marketing), and this communication must comply with the requirements of Article 12

[…]. The information contained in the privacy notice or statement

stating that the data subject should regularly check the notice or statement

on privacy in order to find out about any changes or updates are

considered not only insufficient. »40

It recalls that "the data controller should also, when notifying

changes to the persons concerned, explain to them the impact that these

modifications might have on them. »41

31. The Restricted Committee notes that, even if it appears from the investigation report that the

controlled had planned to inform users by email in the event of a future update of the

privacy policy42, said policy mentioned that “[…]”43

38 Investigation report, page 34, point “4.4.4.3.3 Contradictory information”.

39 Statement of Objections, point 26.

40 WP 260 rev.01, points 11 and 29.

41 WP 260 rev. 01, item 31.

42 Investigation report, page 33, point “4.4.4.2.5 Test 5”.

43 See Exhibit 1 appended to the investigation report, point "[...]".

According to the privacy policy, users were therefore not systematically

actively informed in the event of a substantial modification of said policy.

32. It therefore considers that there was a lack of control at the start of the CNPD's investigation the obligation of transparency arising from Article 12.1 of the GDPR, and more specifically to the requirement to provide the required information in an easily accessible manner.

2.3. As for the requirements to provide information in a way that is "understandable" and "in clear and simple terms"

2.3.1 At the translation level

33. In the context of objective 544 the head of investigation expected, among other things, that "the data protection policy is available in the same languages as those offered on the website, i.e. the languages of the customers targeted by the services of the controlled (cf. Test 3)»45.

CNPD officials then inspected "the data protection policy to identify the existence of a translation in the same languages as those for which the site is available. »46

34. From the statement of objections it is apparent in this context that "CNPD officials found that the policy only exists in French although the site is available in German and French."47

Thus, the head of investigation held that the conditions of article 12.1 of the GDPR with regard to the comprehensibility of the information (at the translation level) have not been respected.48

35. The Restricted Committee recalls that Article 12.1 of the GDPR requires, among other things, that required information must be provided in an understandable way. She notes that the Transparency Guidelines state that "the requirement that such information be "understandable" means that they should be able to be understood by the

44 "Objective 5 - Ensure that information is concise, transparent, understandable, and transmitted in clear and simple terms"; Investigation report, page 37 et seq.

45 Investigation report, page 36, Ad Objective 5, point “4.4.5.1 Expectations”.

46 Investigation report, page 37, Ad Objective 5, point “4.4.5.2.3 Test 3 Translation”.

47 Statement of Objections, paragraph 30

48 Statement of Objections, paragraph 32.

---

majority of the target audience. Comprehensibility is closely linked to the requirement to use plain and simple terms. A controller knows the people about from which it collects information and can use this knowledge to determine what this audience would be likely to understand. »49

36. With regard to the above requirement to provide the information requested in Plain and simple terms, the Transparency Guidelines indicate more specifically that a “translation into one or more languages should be provided when the data controller targets data subjects who speak these LANGUAGES. »50

37. The Restricted Panel therefore considers that, as the audited website was available in French and German, the control should have provided versions of the policy of confidentiality in these two languages. However, said policy was only available in French. Since the auditee had therefore not provided German-speaking users of its site internet a privacy policy in German, he had not provided them with the information required in an easily understandable form.

38. In view of the foregoing, the Restricted Panel concurs with the opinion of the head of investigation and concludes that at the start of the CNPD's investigation, the control failed in the obligation to transparency arising from Article 12.1 of the GDPR, and more specifically from the requirements of

provide the required information in a way that is understandable and in terms that are clear and simple.

2.3.2. At recipient level

39. With regard to objective 551, the head of investigation recalled the information relating to recipients or categories of recipients that must be provided under articles 13 and 14 GDPR according to the Annex to the Transparency Guidelines.

CNPD officers then inspected the privacy policy of the auditee and "noted that certain information described in the data protection policy lacked transparency:

49 WP 260 rev.01, point 9.

50 WP 260 rev.01, point 13.

51 "Objective 5 - Ensure that information is concise, transparent, understandable, and transmitted in clear and simple terms"; Investigation report, page 35 et seq.

- The identity of the sub-contractors of Company A (the recipients of the data) is not specified in the data protection policy. […]. »52

40. In the statement of objections, it is specified by the head of investigation that the "officers of the CNPD noted that the information relating to subcontractors is not sufficiently precise. Indeed, the data protection policy indicates that "[...]".

The identity of Company A's subcontractors (or at least a list of the various categories of subcontractors) is not specified in the policy, so it is difficult for data subjects to understand who holds their data. »

For this reason, the head of investigation was of the opinion that "the conditions of article 12,

paragraph 1 of the GDPR as to the comprehensibility of the information (at the level

addressees) have not been complied with".53

41. The Restricted Panel reiterates that Article 12.1 of the GDPR requires, among other things, that

required information must be provided in an understandable way. She notes that

the Transparency Guidelines state that "the requirement that such information

be "understandable" means that they should be able to be understood by the

majority of the target audience. Comprehensibility is closely linked to the requirement to use

plain and simple terms. A controller knows the people about

from which it collects information and can use this knowledge to

determine what this audience would be likely to understand. »54

It also recalls that in accordance with Article 4.9) of the GDPR, the recipient aims:

"the natural or legal person, public authority, agency or any other body

who receives communication of personal data, whether or not it is a

third. (…)".

WP 260 specifies in this context that a "recipient is not necessarily a

third. Therefore, other controllers, joint controllers of the

processing and subcontractors to whom the data is transferred or communicated are

52 Investigation report, page 37, point "4.4.5.2.1 Test 1: Concise and transparent".

53 Statement of Objections, points 35 and 38.

54 WP 260 rev.01, point 9.

covered by the term "recipient" and information relating to these recipients

should be provided in addition to information about other third party recipients. »55

Pursuant to Article 13.1.e) of the GDPR, the controller must also, where appropriate, provide information on the recipients or information on the categories of recipients of the personal data, and that in this respect the guidelines on transparency specify, among other things, that "the actual recipients (namely designated) of the personal data or the categories of recipients must be indicated. In accordance with the principle of fairness, data controllers must provide data subjects with the most significant information about the recipients. In practice, these are generally named recipients so that data subjects can know exactly who holds their data of a personal nature. If data controllers choose to communicate the categories of recipients, the information should be as specific as possible and indicate the type of recipient (based on the activities they carry out), industry, sector and sub-sector as well as location of recipients."56

42. The Restricted Committee notes in this context that section […] of the policy of confidentiality of the control mentioned that each "[...]". It therefore follows from the said policy that personal data of users could be transmitted to recipients in the context of payments and deliveries.

Nevertheless, according to the register of the controlled57 there were, in addition to the two categories of recipients of the personal data of website users mentioned in the privacy policy, three other categories of recipients: a database hosting provider of Company A named […], the […] and a mailing service provider named […].

43. It therefore considers that the auditee had not provided users of its website with a complete information on the categories of recipients of their personal data staff.

55 WP 260 rev.01, Annex "Information to be communicated to a data subject under Article

13 or section 14”.

56 WP 260 rev.01, Appendix “Information to be communicated to a data subject under Article

13 or section 14”.

57 Exhibit 9 attached to the investigation report. See in particular the sheets […].

---

44. In view of the foregoing, the Restricted Panel agrees with the opinion of the head of investigation and concludes that at the start of the CNPD's investigation, the control failed in the obligation to transparency arising from Article 12.1 of the GDPR and with regard to Article 13.1.e) of the GDPR, and more specifically the requirements to provide the information required from a comprehensible way and in clear and simple terms.

B. On the breach of the obligation to inform the persons concerned

1. On the principles

45. Article 13 of the GDPR provides the following:

“1. Where personal data relating to a data subject is

collected from this person, the data controller provides him, at the time

where the data in question is obtained, all of the following information:

a) the identity and contact details of the controller and, where applicable, of the

representative of the controller;

b) where applicable, the contact details of the data protection officer;

c) the purposes of the processing for which the personal data are intended as well as

the legal basis for the processing;

d) where the processing is based on Article 6(1)(f), the legitimate interests

sued by the controller or by a third party;

e) the recipients or categories of recipients of the personal data,

if they exist; And

(f) where applicable, the fact that the controller intends to carry out a

transfer of personal data to a third country or to an organization

international community, and the existence or absence of an adequacy decision issued by the

Commission or, in the case of transfers referred to in Article 46 or 47, or Article 49,

paragraph 1, second subparagraph, the reference to the appropriate or suitable safeguards and the

means of obtaining a copy or where they have been made available;

2. In addition to the information referred to in paragraph 1, the controller shall provide the

the data subject, at the time the personal data is obtained,

---

the following additional information which is necessary to guarantee a

fair and transparent treatment:

a) the retention period of the personal data or, where this is not

possible, the criteria used to determine this duration;

b) the existence of the right to request from the controller access to the data to

personal character, the rectification or erasure of these, or a limitation of the

processing relating to the data subject, or the right to oppose the processing and

right to data portability;

c) where the processing is based on point (a) of Article 6(1) or on Article 9,

paragraph 2(a), the existence of the right to withdraw consent at any time,

without affecting the lawfulness of the processing based on the consent made before the

withdrawal thereof;

d) the right to lodge a complaint with a supervisory authority;

(e) information on whether the requirement to provide data to

personal nature has a regulatory or contractual nature or if it conditions the

conclusion of a contract and whether the data subject is obliged to provide the data to

personal character, as well as on the possible consequences of the non-provision of

those data ;

f) the existence of automated decision-making, including profiling, referred to in Article

22, paragraphs 1 and 4, and, at least in such cases, useful information concerning the

underlying logic, as well as the significance and intended consequences of such processing

for the person concerned.

3. When he intends to carry out further processing of personal data

personal data for a purpose other than that for which the personal data

have been collected, the data controller provides the data subject beforehand

concerned information about this other purpose and any other information

relevant referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 do not apply where and to the extent that the person

concerned already has this information. »

---

46. The communication to data subjects of information relating to the processing of

their data is an essential element in the context of compliance with the general obligations

of transparency within the meaning of the GDPR.58 These obligations were clarified by the Group

of Article 29 in its guidelines on transparency which have been taken up and

re-approved by the EDPS.

47. For the rest, the Restricted Panel refers to points 12 to 15 of this

decision with regard to the principles to be observed under the obligation to

transparency in accordance with Article 12.1 of the GDPR.

2. In this case

48. In the context of objective 259 the head of investigation expected, among other things, that “the

following information is accessible through the data protection policy,

in accordance with the appendix to the guidance of the Article 29 Working Party on

information to be communicated to a data subject under Article 13

or Article 14 of the GDPR:

[…] - The purpose(s) and legal basis of the processing (it is expected that the legal basis

specific to the treatment is filled in and not simply the list of databases

that exist under the GDPR) (cf. Test 3), […]

- Transfers to third countries where applicable (see Tests 7 and 19), […]

- The rights of data subjects: […] right to withdraw consent at any time

moment. […]. »

49. As a preliminary point, with regard to the information on the legal bases of cookies

and their transfer to third countries, the Restricted Training wishes to specify that as the

control of the application and compliance with the amended law of May 30, 2005 was not within the

scope of the investigation in question, the Restricted Panel does not rule in this

decision on the compliance of the audit with the requirements of this law.

58 See in particular Articles 5.1.a) and 12 of the GDPR, see also recital (39) of the GDPR.

59 “Objective 2 - Ensure information is complete”; Investigation report, page 15 et seq.

2.1. As to the legal bases of the processing

50. It appears from the investigation report that even if “the processing purposes are clearly mentioned in the data protection policy, the legal bases are not indicated, neither in the policy (PIECE 1), nor in the processing register (PIECE 9). »60

For these reasons, the head of investigation noted in the statement of objections that "the conditions of Article 13, paragraph 1, letter c) of the GDPR with regard to the legal bases of treatments have not been followed. »61

51. The Restricted Committee notes that the legal bases for the processing of data was not indicated in the privacy policy or in the register of the control.

The controller has therefore not provided users of its website with all the information made mandatory by Article 13.1.c) of the GDPR.

2.2. Regarding data transfers to a third country

52. CNPD officials noted that in the privacy policy, the control “does not indicate transferring personal data to third countries or international organizations (PIECE 1, pages 2 and 3).

However, CNPD officials noted, during interviews with the Company A, that data was transferred to […] (online payment provider, […]) and to […] (email service provider […]). […] So there are many transfers to third countries, which are not mentioned in the data protection policy data. »62

For these reasons, the head of investigation noted in the statement of objections that "the conditions of Article 13, paragraph 1, letter f) of the GDPR with regard to information on data transfers to third countries have not been respected. »63

60 Investigation report, page 17, point “4.4.2.2.3 Test 3: Purposes and legal bases”.

61 Statement of Objections, point 47.

62 Investigation report, page 19, point "4.4.2.2.7 Test 7: Transfers to third countries - register".

63 Statement of Objections, point 51.

---

53. The Restricted Committee indeed notes that the confidentiality policy indicated that the controlled “does not transfer personal data to a third country, nor to a international organization”64, while it appears from the Minutes65, as well as from the record of the control that personal data was transferred [to third countries] to its online payment ([…]) and e-mail ([…]) providers.
The controller has therefore not provided users of its website with all the information made mandatory by Article 13.1.f) of the GDPR.

2.3. As to the right to withdraw consent

54. CNPD officers inspected the auditee's privacy policy to identify the presence of information relating to the rights of data subjects including a summary of what the rights include and what action can be taken by the data subject to exercise them as well as any limitation to said rights.66
They noted in this context "that consent was requested for the sending of newsletters when registering a new customer. At this level, there is a link to the data protection policy, but the policy does not mention the right for a user to withdraw consent at any time. »67

55. The head of investigation took into account in the statement of objections "that the user may change their consent to send newsletters at any time by changing their account settings. He can also unsubscribe from the newsletters by clicking on the unsubscribe link at the bottom of the email. »

It nevertheless held that "the conditions of Article 13, paragraph 2, letter c) of the

GDPR regarding the information on the right to withdraw consent have not been

respected. »68

56. The Restricted Committee recalls that the obligation to mention the existence of the right to

withdrawing consent at any time is only necessary when the processing by the

64 Privacy Policy, page 3.

65 See page 5 which states the following: “Company A uses the following subcontractors: […] - […] (payments

on line, […]) ; - […] (email service provider, […]) […]. »

66 Investigation report, page 20, point “4.4.2.2.9 Test 9: Rights of data subjects (users)”.

67 Statement of Objections, point 54.

68 Statement of Objections, points 55 and 56.

controller is based on Article 6.1.a) or 9.2.a) of the GDPR, i.e. if

the legal basis for processing is the consent of the data subject.

In the present case, as indicated in point 51 of this decision, neither the policy of

confidentiality, nor the audited register mentioned the legal bases of the different

treatments performed. The Restricted Committee nevertheless notes that it was documented by

a screenshot sent by the controlled only when a user wanted to create a

account, he had to actively tick a box if he wanted to receive the newsletter.69

elsewhere, other screenshots sent by the controlled showed the possibility for

a user to actively subscribe on the website of the controlled to his newsletter and

that in this case, an email confirming registration on the newsletter mailing list

was sent to him.70

Based on the foregoing, the Restricted Panel concludes that the legal basis of the processing of personal data carried out in the context of sending the newsletter was the consent of the user and that therefore the control was obliged to inform said user of the existence of the right to withdraw his consent to any moment.

57. In this case, the Restricted Panel notes that when creating an account by a user, a link to the privacy policy was available. However, although a user could always modify their consent relating to the sending of the newsletter by changing the parameters of his account71, said policy did not mention not the existence of the right to withdraw consent at any time.

Furthermore, in the event that a user actively subscribes to the website of the controlled to its newsletter, no information on the existence of the right to withdraw consent to any time was available to him, neither at the time of registration on the website, nor when he received the email confirming subscription to the newsletter mailing list. He could nevertheless unsubscribe from the newsletter by clicking on the unsubscribe link found at the bottom of the email sending said newsletter.

69 See Exhibit 5 attached to the investigation report.

70 See Exhibit 7 attached to the investigation report.

71 See statement of objections, paragraph 55.

58. The auditee therefore did not provide users of its website with all the information made mandatory by Article 13.2.c) of the GDPR.

59. In view of the foregoing in points 50 to 58, the Restricted Panel agrees with the opinion of the

head of investigation and concludes that at the start of the CNPD investigation, the control failed to its obligation to inform data subjects arising from Article 13.1.c), f) and 13.2.c) of the GDPR, and more specifically to inform them about the legal bases of the processing, on transfers of personal data to third countries or international organizations, as well as the existence of the right to withdraw their consent at any time.

II. 2. On the fine and corrective measures

1. On the principles

60. In accordance with article 12 of the law of 1 August 2018, 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 the envisaged processing are likely to violate the provisions of this Regulation;

(b) call a controller or processor to order when the processing operations have resulted in a breach of the provisions of this Regulation;

(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, of specific manner 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 restriction, including prohibition, of the processing;

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 penalty under section 83, in addition to or in addition to
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. »

61. In accordance with article 48 of the law of 1 August 2018, the CNPD may impose fines
administrative as provided for in Article 83 of the GDPR, except against the State or
of the municipalities.

62. 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".

63. 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. The possible

changes relating to the data processing under investigation

subsequently, even if they make it possible to establish in whole or in part the

conformity, do not make it possible to retroactively cancel a breach noted.

64. 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 as part of any corrective measures to be taken

and/or setting the amount of any administrative fine to be imposed.

---

2. In this case

2.1. Regarding the imposition of an administrative fine

65. In the statement of objections, the head of investigation proposes to the Restricted Panel to

pronounce against the controlled an administrative fine relating to the amount of

1,700 euros.

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

applicable, of the amount of this fine, the Restricted Panel analyzes the criteria set

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

concerns breaches of Articles 12 and 13 of the GDPR, it recalls that

information and transparency relating to the processing of personal data

personnel are essential obligations weighing on data controllers

so that people are fully aware of the use that will be made of

their personal data, once collected. A breach of

articles 12.1 and 13 of the GDPR thus constitute an infringement of the rights of individuals concerned. The right to transparency and the right to information have also been reinforced under the GDPR, which demonstrates their particular importance.

- As for the duration criterion (article 83.2.a) of the GDPR), the Restricted Panel finds that these shortcomings have lasted over time, at least since the beginning of the CNPD investigation and until, where applicable, a possible modification of the data protection policy. She recalls that guidance relating to principles and obligations provided for in the GDPR was available from the CNPD, especially on its website.

- As for the number of data subjects (article 83.2. a) of the GDPR), the Training Restreinte notes that it is […]. The controller specified that in 2020 approximately […] orders were carried out by […].72

- As to whether the breaches were committed deliberately or not (by negligence) (article 83.2.b) of the GDPR), the Restricted Panel recalls that "no deliberately" means that there was no intention to commit the violation, although

72 See minutes, pages 4 and 6.

the controller or the processor has not complied with the obligation to due diligence required by law.

In this case, the Restricted Committee is of the opinion that the facts and breaches observed do not reflect a deliberate intention to violate the GDPR on the part of the control.

- As to the degree of cooperation established with the supervisory authority (Article 83.2. f) of the GDPR), the Restricted Panel takes into account the statement of the head of investigation according to which the auditee has shown constructive participation throughout investigation.73

- As for the measures taken by the inspected party to mitigate the damage suffered by the persons concerned (article 83.2.c), the Restricted Training takes into account the measures taken by the auditee and refers to Chapter II.2. Section 2.2. of this decision for the related explanations.

67. 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.

68. It also notes that while several measures have been put in place by the control in order to remedy in whole or in part certain shortcomings, these were only adopted following the launch of the investigation by CNPD agents on August 26, 2020 (see also point 63 of this decision).

69. Therefore, the Restricted Panel 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 12.1 and 13 of the GDPR.

70. With regard to the amount of the administrative fine, the Restricted Committee recalls that the paragraph 3 of Article 83 of the GDPR provides that in the event of multiple infringements, such as this is the case here, the total amount of the fine may not exceed the amount set for the most serious violation. To the extent that a breach of Articles 12.1 and 13 of the GDPR is blamed on the controlled, the maximum amount of the fine that can be withheld

73 Statement of Objections, point 60.c).

Survey no. […] conducted with Company A.

amounts to 20 million euros or 4% of worldwide annual turnover, whichever is the greater

high being retained.

71. In view of the relevant criteria of Article 83.2 of the GDPR mentioned above, the Training

Restricted considers that the pronouncement of a fine of one thousand four hundred (1,400) euros

appears to be both effective, proportionate and dissuasive, in accordance with the requirements of

GDPR Article 83.1.

2.2 Regarding the taking of corrective measures

72. In the statement of objections, the head of investigation proposes to the Restricted Panel

to adopt the following corrective measures: “within a period of 1 month from the

notification to Control of the decision taken by the Restricted Training:

Order, pursuant to Article 58 (2) d) of the GDPR, the Controlled to comply with

Article 12 (1) of the GDPR by making the following changes:

a) Update the data protection policy and the cookies policy of the

Company A by ensuring that the information contained in these policies reflects

the reality, in particular at the level of the use of the technique of profiling,

the existence of a DPD and retention periods for cookies and controls

client ;

b) Adapt in the data protection policy the information relating to its implementation

up to date ;

c) Translate the data protection policy into the same languages as those

proposed for the website;

d) Specify in the data protection policy the information on the

data recipients.

Order, pursuant to Article 58 (2) d) of the GDPR, the Controlled to comply with

Article 13 paragraphs (1) and (2) of the GDPR, by informing, in the protection policy

data, the following information:

- the legal bases for data processing and cookies;

- information relating to data transfers to third countries;

- information on the right to withdraw consent at any time."74

73. On a preliminary basis, with regard to the corrective measures proposed by Chief

of investigation concerning the cookies deposited by the controlled party, the Restricted Training

reiterate that as the control of the application and compliance with the amended law of May 30

2005 was not within the scope of the investigation in question, the Restricted Panel does not rule

not in this decision on the corrective measures proposed by the Chief

of investigation concerning the cookies deposited by the controlled.

74. As for the other corrective measures proposed by the head of investigation and by reference

in point 64 of this decision, the Restricted Panel takes into account the

steps taken by the controller to comply with the provisions of articles

12.1 and 13 of the GDPR, as detailed in particular in its letter of February 10, 2022.

More specifically, it takes note of the following facts:

- As for the corrective measure proposed by the head of investigation mentioned under a) of point

72 of this decision regarding the update of the privacy policy in

ensuring that the information reflects reality, particularly in terms of use

the profiling technique, the existence of a DPO and the retention periods of the

customer orders, Restricted Training takes into account the accuracy of the

verified during the meeting of July 13, 2022 that the privacy policy has been updated

updated on February 17, 2022 (hereinafter: “the updated privacy policy”) and

that it has already been put on its website.

In its letter of February 10, 2022, the auditee specified that it had updated its policy

of confidentiality by "removing references to profiling techniques that

we do not apply. In section […]75 of the updated Privacy Policy

there is no longer any mention of a profiling technique. On the contrary, she

notes that the updated privacy policy still mentions in the part

[…] that “Company A collects and processes in particular the […] preferences and centers

interests […] of the Users. » The Restricted Committee therefore considers that the collection

of the aforementioned data always implicitly refers to the use of a

profiling technique.

74 Statement of Objections, point 58.

75 Part […] in the former privacy policy.

Furthermore, in the said letter of February 10, 2022, the controller specified that he had updated

the “information, including contact details, relating to the DPO, post that

we introduced in 2021.” The updated privacy policy mentions

therefore that the controlled "has appointed a Data Protection Officer

(DPO) who can be contacted at the following email address: […]”. During the hearing of the

Restricted training of July 13, 2022, the audit confirmed the appointment of a DPO

internal who also has other tasks.

Finally, with regard to the retention periods for customer orders, the

Restricted Training notes that the updated privacy policy contains a

specific section on data retention periods76 indicating that if [a
customer requests the closure of his account, his personal data is deleted
or made anonymous]. In this part the user is also invited to consult
the retention period of personal data per processing in the tables
described in part […] of its policy. By reviewing the retention periods of
various data processed as part of the "[…]" processing indicated in these
tables, the Restricted Committee finds that the "personal data" and the
"order data"77 are saved for ten years. He is not there
indicated that the personal data will be deleted or made anonymous if
the user requests the closure of his account.

There is therefore an inconsistency between the […] part of the updated privacy policy.
day and the retention periods indicated in part […].

In view of the insufficient compliance measures taken by the control
in this case and point 64 of this decision, the Restricted Panel considers
as soon as it is necessary to pronounce the corrective measure proposed by the head of investigation
in this regard and taken up in point 72 of this Decision under (a) concerning the duration
retention of customer orders, as well as reference to the use of the
profiling technique.

- As for the corrective measure proposed by the head of investigation mentioned under b) of point
72 of this decision concerning the information relating to the update of the
privacy policy, the controlled confirmed in his letter of February 10, 2022

76 See part […]

77 By "Personal data:" is meant […] and by "Order data" […].

have adapted the privacy policy and more specifically “the information relating to

its update by specifying that registered users are informed of any

change by e-mail. »

The Restricted Training notes that the updated privacy policy mentions

in part […] that [registered customers are informed of any change in the

Email Privacy Policy].

In consideration of the sufficient compliance measures taken by the control

in this case and point 64 of this decision, the Restricted Panel considers

when there is no reason to pronounce the corrective measure proposed by the chief

investigation in this regard and taken up in point 72 of this decision under b).

- As for the corrective measure proposed by the head of investigation mentioned under c) of point

72 of this decision regarding the translation of the privacy policy

in the same languages as those proposed for the website, the controller indicated

in his letter of February 10, 2022 that “on […] 2022, we published the

German data protection policy. »

Indeed, the Restricted Committee finds that the privacy policy is

now available in the same languages as the audited website, i.e.

say in French and German.

In consideration of the sufficient compliance measures taken by the control

in this case and point 64 of this decision, the Restricted Panel considers

when there is no reason to pronounce the corrective measure proposed by the chief

investigation in this regard and taken up in point 72 of this decision under c).

- As for the corrective measure proposed by the head of investigation mentioned under d) of point

72 of this decision regarding clarification in the privacy policy

information on the recipients of the data, the controller has indicated in his

letter of February 10, 2022 that “as of […] 2022, we updated the policy

data protection by specifying the information on the recipients of the data

and more particularly the category of recipients. »

- By reading the updated privacy policy, the Restricted Training finds that

in part […] the recipients of the data, named according to the

different treatments, are specified, while part […] contains [a list of the

entities authorized to receive personal data relating to the client].78

In consideration of the sufficient compliance measures taken by the control

in this case and point 64 of this decision, the Restricted Panel considers

when there is no reason to pronounce the corrective measure proposed by the chief

investigation in this regard and taken up in paragraph 72 of this Decision under (d).

- As for the corrective measures proposed by the head of investigation included in the second

paragraph of point 72 of this decision concerning the inclusion in the policy of

confidentiality of information on the legal bases of data processing, on

data transfers to third countries, as well as information relating to the right to

withdraw its consent at any time, the control indicated in its letter of 10

February 2022 as follows: […] dated […] 2021:

- we have added the legal bases for data processing;

[…]

- we have added the information relating to the right to withdraw consent at any time

moment.

Please note that an additional update is planned soon in order to:

[…]

- further specify transfers to third countries, in particular in relation to the

payment platform […] and the newsletter management solution […]. »

With regard to the legal bases of data processing, the Training

Restricted notes that in part […] of the Privacy Policy, the basics

legal are mentioned by data processing. About the

treatment referred to as "[...]", it nevertheless notes that two different bases

are indicated,79 while the data controller can only rely on

on one of the six legal bases provided for in Article 6 of the GDPR. The EDPS clarified in

this context in its consent guidelines the following: “Article 6

78 And more specifically […] (Electronic payment service provider), […] (Publisher […] of Company A),

[…] (Delivery service provider), […] (Database hosting provider), […] (Partner

[…]).

79 And more specifically: “[…]”.

establishes the conditions for lawful processing of personal data and describes

six legal bases on which a data controller can rely.

The application of one of these six legal bases must be established before the activity of

processing and in connection with a specific purpose. »80

With regard to information relating to the right to withdraw consent at any time

moment, the Restricted Committee would like to refer to point 56 of this decision

by reiterating that the obligation to mention the existence of the right to withdraw

consent at any time is only required if the legal basis for the processing

is the consent of the data subject, i.e. in this case the sending of the

newsletter by the controlled.

She notes that in part […] is mentioned the following: “[…].” Training

Restreinte considers in this context that the controlled has made an amalgam of two bases

legal and two different data processing: the consent of the

the user for sending the newsletter, a consent that the data subject

must be able to withdraw at any time, on the one hand, and the execution of the contract between the controlled

and users with regard to the management of orders […], a contract that

users can terminate by closing their account, on the other hand. It is important

to note in this context that "consent cannot be obtained by

same action as when a data subject accepts a contract or the conditions

general of a service. The global acceptance of the general conditions cannot be

considered as a clear affirmative act aimed at giving consent to the use

of personal data. »81

The privacy policy must therefore mention more precisely that the user

has the right to withdraw at any time his consent given for the sending of the

newsletter.

With regard to transfers to third countries, the Restricted Committee notes that

the updated privacy policy states in part […] the following: “To

processors/tools […] and […], a transfer of data takes place to third countries.

[…]”.

80 EDPS Guidelines 5/2020 on consent within the meaning of Regulation (EU) 2016/679, Version 1.1,

Adopted on 4 May 2020, point 121.

81 EDPS Guidelines 5/2020 on consent within the meaning of Regulation (EU) 2016/679, Version 1.1,

Adopted on 4 May 2020, point 81.

However, as Article 13.1.f) of the GDPR requires the controller to
mention "the intention to transfer personal data to
a third country or an international organisation, and the existence or absence of a
adequacy decision issued by the Commission or, in the case of the transfers referred to
in Article 46 or 47, or in the second subparagraph of Article 49(1), the reference to the
appropriate or suitable warranties and the means of obtaining a copy thereof or the place
where they have been made available", the Restricted Committee considers that the
information provided by the controller is not sufficient […].

In view of the insufficient compliance measures taken by the
controlled in this case and point 64 of this decision, the Restricted Panel
therefore considers that the corrective measures proposed by
the head of investigation in this regard and included in the second paragraph of point 72 of this
decision concerning the insertion in the privacy policy of information on the
legal bases for data processing, on transfers of data to
third countries, as well as information on the right to withdraw consent to any
moment.

In view of the foregoing developments, the National Commission sitting
in restricted formation and after having deliberated, decides:

- to retain breaches of Articles 12.1 and 13 of the GDPR;
- impose an administrative fine on Company A in the amount of
one thousand four hundred (1,400) euros, with regard to the breaches constituted in articles 12.1
and 13 GDPR;
- issue against Company A an injunction to bring the

processing with the obligations resulting from article 12.1 of the GDPR, within a period of 2 (two) months following the notification of the decision of the Restricted Panel, and, in particular :

o update in the confidentiality policy the retention periods of the personal data collected in the context of orders from customers by ensuring that their indication is consistent in the different parts of said policy;

---

o ensure that the information contained in the privacy policy reflect reality in the use of profiling techniques;

- issue an injunction against Company A to bring the processing with the obligations resulting from Article 13 of the GDPR, within 2 (two) months following the notification of the decision of the Restricted Panel, and, in particular :

o update in the privacy policy the legal bases of the different data processing operations by ensuring that a single legal basis per treatment is mentioned;

o update the privacy policy by mentioning the right for a user to withdraw at any time his consent given for the sending of the newsletters;

o update in the privacy policy the information on the data transfers to third countries.

Belvaux, December 13, 2022.

For the National Commission for Data Protection sitting in restricted formation

Tine A. Larsen Thierry Lallemang

President

Commissioner

Alain Hermann

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.
