Decision of the National Commission sitting in restricted formation

on the outcome of investigation No. […] conducted with Company A

Deliberation No. 31FR/2021 of August 5, 2021

The National Commission for Data Protection sitting in restricted formation

composed of Ms. Tine A. Larsen, President, and Messrs. Thierry Lallemang and

Christophe Buschmann, curators;

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

on the protection of individuals with regard to the processing of personal data

personal character and on the free movement of such data, and repealing Directive

95/46/EC;

Considering the law of August 1, 2018 on the organization of the National Commission for the

data protection and the general data protection regime, in particular

its article 41;

Having regard to the internal regulations of the National Commission for the Protection of

data 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

inquiry 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. As of May 20, 2019, the National Data Protection Commission

(hereafter: the “CNPD”) received a complaint from […] (hereafter: “the complainant”)

brought against Company A. The latter informed the CNPD that letters

electronic data including medical data, as well as indications and

sensitive questions relating to his state of health, written by his insurance and which

were intended, would have been sent to third party recipients.

2. More specifically, the Claimant asserted that on October 19, 2018, a

employee of Company A would have sent an e-mail to the e-mail address "[...]",

while his correct email address would be "[...]". This email included in the body

of the text, among other things, the surname of the claimant, his sex, as well as indications

details on certain pathologies. Attached to that e-mail were three

separate forms, to be completed by the claimant, relating to the pathologies that the claimant has

declared to his insurance in the context of obtaining life insurance. 7

November 2018, the employee of Company A did inform the claimant by e-

email that the aforementioned email of October 19, 2018 had been sent to a

wrong address.

3. The Claimant further specified that on November 29, 2018, a second

e-mail would have been sent by the same employee of Company A to the address

e-mail "[...]" and which included in the body of the text his surname, questions

very precise as to a specific pathology, the family name of the doctor of

life insurance, an indication of the address of the said doctor, as well as two non-

filled in referencing said pathology and intended to be filled out by him or his doctor.

4. By e-mail of December 3, 2018, Company A again contacted by e-mail the

claimant and informed him that repetitive erroneous sendings had taken place and that the delegate to

Data Protection (hereinafter: "DPD") of the insurance has been notified. It is specified there

also that all measures will be taken to avoid such incidents in the future.

5. During its deliberation session on June 5, 2019, the National Commission for

data protection sitting in plenary session (hereafter: “Training

Plenary”) therefore decided to open an investigation with Company A on the basis of

article 37 of the law of 1 August 2018 on the organization of the National Commission for

_____

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

Survey no. […] conducted with Company A.

2/41

data protection and the general data protection regime (hereinafter:

“Law of August 1, 2018”) and to appoint Mr. Marc Lemmer as head of investigation.

6. According to the decision of the Plenary Formation, the investigation conducted by the CNPD

was intended to verify compliance with the provisions of Regulation (EU) 2016/679 of the

European Parliament and of the Council of 27 April 2016 on the protection of persons

physical with regard to the processing of personal data and to the free

circulation of this data, and repealing Directive 95/46/EC (hereinafter: “GDPR”) and

of the law of August 1, 2018.

7. On July 19, 2019, CNPD agents carried out a visit to the

the premises of Company A. Given that the minutes relating to the said mission

on-site investigation only mentions as responsible for the controlled processing the

Company A,1 the decision of the National Commission for Data Protection

sitting in a restricted formation on the outcome of the investigation (hereinafter: “Formation

Restricted”) will be limited to processing controlled by CNPD agents and carried out

by Company A.

8. Company A is a […] registered in the Trade and Companies Register of

Luxembourg under number B […] and having its registered office […] (hereinafter “the controlled”).

The audit [aims to carry out all insurance and reinsurance operations of the

“Life” branch […]. » 2

9. As of July 23, 2019, the audited has sent details of the issues

requested by CNPD officials during their on-site visit and concerning the

possibility to speak to the DPO, as well as on the internal register of data breaches at

personal character. Copies of the disputed e-mails were also

attached to said letter.

10. By letter dated August 8, 2019, the controller responded to the report drawn up by

CNPD officials, as well as additional questions asked by mail from the

CNPD of July 29, 2019.

1 See in particular Minutes no. […]/2019 relating to the on-site fact-finding mission carried out on

July 19, 2019 with Company A.

2 According to the statutes coordinated at […].

11. By letter dated September 17, 2019, the controller answered the questions

additional questions asked by letter from the CNPD of September 5, 2019.

12. At the end of his investigation, the head of investigation notified the person inspected on 29

October 2019 a statement of objections detailing the shortcomings he considered

constituted in this case, and more specifically a non-compliance with the requirements prescribed

by Articles 5.1.f), 32.1. a) and b), 33.1, 33.5, 34.1 and 37.7 GDPR.

13. On November 29, 2019, the auditee produced written observations on the

statement of objections.

14. A supplementary letter to the statement of objections was sent to the

checked on December 15, 2020. In this letter, the head of investigation proposed to

the Restricted Formation to adopt five different corrective measures, as well as to inflict

to the control an administrative fine of 275,000 euros.

15. By letter dated January 27, 2021, the controller produced written observations

on the supplementary letter to the statement of objections.

16. The president of the Restricted Formation informed the controller by letter of 29

April 2021 that his case would be registered for the Restricted Panel session of July 14

2021. The controller confirmed his presence at the said meeting on June 1, 2021.

17. During the Restricted Training session of July 14, 2021, the head of investigation

and the controller presented their oral observations in support of their written observations

and answered the questions posed by the Restricted Panel. The control had the

speak last.

II. Place

II. 1. As to the reasons for the decision

A. On the breach of the obligation to document a data breach at

personal character

1. On the principles

18. According to the provisions of Article 33.5 of the GDPR, the controller

is obliged to document “any personal data breach, indicating

the facts about the personal data breach, its effects and the

measures taken to remedy it. » The documentation thus compiled allows the authority

control to verify compliance with this article.

19. The obligation to document a data breach also arises from the

principle of responsibility (“accountability”) set out in articles 5.2 and 24 of the GDPR

requiring the controller to implement technical and

organizational arrangements to ensure and be able to demonstrate that the

processing is carried out in accordance with the GDPR.

20. The obligations in this area have been clarified by the Working Group Article

29 in its Data Breach Notification Guidelines

personnel under Regulation (EU) 2016/679 (hereinafter: “WP 250rev.01”).

21. It should be noted that the European Data Protection Board (hereinafter:

“EDPS”), which has replaced the Article 29 Working Party since 25 May 2018, took over

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

2018, such as in particular the said guidelines.3

22. The data controller may decide to document breaches in the

framework of its register of processing activities kept in accordance with Article 30 of the

GDPR. A separate register is not necessary, provided that the information

concerning the violations are clearly identifiable as such and can be

retrieved on request.4 While it is therefore up to the controller to determine

the method and structure to be used to document a violation, certain information

keys should be included in all circumstances as required by Article 33.5 of the

GDPR.

3 See EDPS Endorsement Decision 1/2018 of 25 May 2018, available at

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

4 See WP 250rev.01, page 30, footnote 43.

23. WP 250rev.01 further specifies that in the event of “breach of this obligation to properly document a breach, the supervisory authority could exercise its powers under Article 58 and/or impose an administrative fine in accordance with section 83."

24. To trigger the obligation provided for in Article 33.5 of the GDPR, two conditions cumulative must therefore be met:

~ data must be subject to a personal data breach within the meaning of Article 4.12 of the GDPR;

~ these data are to be qualified as personal data within the meaning of Article 4.1 GDPR.

1.1. Regarding the concept of personal data

25. Article 4.1 of the GDPR defines personal data as "any information relating to an identified or identifiable natural person […]; is deemed to be an "identifiable natural person" a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such name, identification number, location data, online identifier, or to one or more specific elements specific to his physical, physiological, genetic, psychic, economic, cultural or social”.

26. According to recital (26) of the GDPR, to “determine whether a person physical is identifiable, it is necessary to take into consideration all the means reasonably likely to be used by the controller or by any other person to identify the natural person directly or indirectly, such as Targeting. To establish whether means are reasonably likely to be used to identify a natural person, it is necessary to take into consideration all

objective factors, such as the cost of identification and the time required for it,

taking into account the technologies available at the time of processing and evolution

of these. »

27. The Article 29 Working Party has considered that “a person may be considered

physical as "identified" when, within a group of people, it

"distinguishes" from all other members of this group. The natural person is therefore

"identifiable" when, even without having yet been identified, it is possible to do so

(as expressed by the “-able” suffix). […] With regard to persons “directly”

identified or identifiable, the name of the person is obviously the identifier most

current and, in practice, the notion of "identified person" most often implies

a reference to that person's name. In order to ensure its identity, the name of the

person must sometimes be associated with other pieces of information (date of birth,

parents' name, address or photo ID) to avoid any confusion between this

person and any namesakes. […] The name can also be the starting point

leading to information about the person's home or whereabouts

and information about his family members (via surname) and

different legal and social relationships associated with this name (education/studies, file

medical, bank accounts). » 5

28. With respect to "indirectly" identified or identifiable persons, the

Article 29 Working Party refers to the “phenomenon of “combinations

unique” to any degree. For cases where, at first glance, the identifiers

are insufficient to enable anyone to distinguish a particular person, that

person can nevertheless be "identifiable", because this information combined with other

items of information (whether these are kept by the person in charge of the

treatment or not) make it possible to distinguish it among other people. » 6

29. The Court of Justice of the European Union (hereafter: “CJEU”) ruled in this

meaning by considering that "the operation consisting in referring, on an Internet page,

to various people and to identify them either by name or by other means, by

example their telephone number or information relating to their conditions of

work and hobbies, constitutes "processing of personal data

automated in whole or in part,” within the meaning of Article 3(1) of Directive

95/46”. 7

5 Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, WP 136, p. 13 and 14.

6 Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, WP 136, p.14.

7 Judgment of 6 November 2003 in case C-101/01 (Lindqvist), point 27. It should be noted that Directive 95/46 was repealed by the GDPR, but the definition of personal data has remained almost identical.

1.2. Regarding the notion of personal data breach

30. Article 4.12 of the GDPR defines a personal data breach

as “a breach of security resulting, accidentally or unlawfully, in the

destruction, loss, alteration, unauthorized disclosure of personal data

personal data transmitted, stored or otherwise processed, or unauthorized access

to such data.

31. WP 250rev.01 (p.7) specifies in this context that “[…] the processing not

authorized or unlawful may include the disclosure of personal data to

recipients (or access to such data by them) not being authorized to

receive (or have access to), or any other form of processing in breach of the GDPR. »

32. Recital (85) of the GDPR details the consequences for data subjects

concerned, because a "breach of personal data risks, if one

fails to intervene in time and in an appropriate manner, to cause natural persons

concerned physical or material damage or moral prejudice such as loss

control over their personal data or the limitation of their rights, a

discrimination, identity theft or theft, financial loss, reversal

unauthorized use of the pseudonymization procedure, damage to reputation, loss

confidentiality of personal data protected by professional secrecy

or any other significant economic or social damage. »

2. In this case

33. During the on-site visit of July 19, 2019, CNPD officials observed

that the register of personal data breaches, created by the controller in

May 2018, did not include any registration.8

34. By letter dated July 23, 2019, the controller confirmed the facts underlying the

complaint received by the CNPD,9 while specifying that in its assessment, the

combination of disclosed data (surname and health conditions) did not allow

8 Findings 3 and 5 of Minutes no. […]/2019 relating to the on-site fact-finding mission carried out on

July 19, 2019 with Company A.

9 See paragraphs 2 to 4 of this decision.

not directly or indirectly identify the claimant. He also claimed to have

contacted the CNPD by telephone in this context and conducted a search on
Internet which would not have displayed any link to the complainant. Therefore, the auditee estimated
that the information disclosed by the two e-mails would not be
qualify as personal data and that therefore, no violation of such
data would not have taken place.10

35. In his letter of September 17, 2019, the auditee also indicated that in
dated December 3, 2018, the “Chief Executive Officer” (hereinafter: “CEO”) and the DPO
been informed of the incidents, while on December 4, 2018 a document […] was drawn up
by the “[…]” and sent to the CEO and the DPO.11

36. The head of the investigation considered, on the other hand, that “the disputed e-mails
disclosed to the wrong recipients clearly include personal data
personal. Thus, the email of October 19, 2018 contained in particular the
Complainant's surname, sex, e-mail address containing an error in
strike, but allowing the first letter of the plaintiff's first name to be deduced, as well as
detailed information on three concrete pathologies with which the plaintiff is afflicted. By
elsewhere, attached to said e-mail were three separate non-secure forms,
completed by the claimant, relating to the pathologies that the latter has declared to the
responsible for processing in the context of obtaining life insurance. These
forms also contained the address of the relevant life insurance company.
While this address information is not personal data per se,
this information (and in particular Luxembourg as the sending country) can be associated
to the complainant for the purpose of identifying him. (Statement of Objections, p.3.)

37. Furthermore, the head of investigation was of the opinion that the sending of e-mails
containing personal data to an incorrect recipient must be qualified
personal data breach, the latter having “resulted, in a manner
accidental disclosure of personal data to third parties

who were not authorized to take cognizance of the information contained in the

e-mails and their attachments. Added to this is the aggravating fact that the data

10 See also the audit letter of November 29, 2019.

11 See Appendices 1 and 2 of the audit letter of September 17, 2019.

disclosed to unauthorized persons were health data with a

particularly "sensitive" nature with regard to the privacy of the person

concerned. He concluded that the auditee did not respect his obligation to document

these two personal data breaches and that therefore it is appropriate to retain

against him a non-compliance with the prescriptions of

GDPR Article 33.5

(Statement of Objections, p.5).

2.1. Regarding the presence of personal data

38. The Restricted Committee first wishes to specify that a natural person

is to be considered as identifiable if information contains elements

identification which can allow him to be identified directly or indirectly. According to

the CJEU, “the use by the Union legislator of the term “indirectly” tends to

indicate that, in order to qualify information as personal data, it is not

it is not necessary that this information, on its own, identify the person

concerned. 12 To the extent that recital (26) of the GDPR refers to the means

likely to be reasonably implemented both by the controller

only by any "other person" to identify the natural person directly or

indirectly, the wording of the latter suggests that, for a datum to be qualified

of “personal data” within the meaning of article 4.1 of the GDPR, “it is not required

that all information allowing the identification of the person concerned must be

find in the hands of one person. »13

39. As mentioned in point 28 of this decision, the Working Group

Article 29 considered that “the natural person is therefore “identifiable” when, even

without having yet been identified, it is possible to do so. […] As regards people “

directly” identified or identifiable, the name of the person is obviously

the most common identifier […]. In order to ensure his identity, the name of the person

must sometimes be associated with other pieces of information […] in order to avoid any confusion

between this person and any namesakes. […] The name can also be the point

of departure leading to information about the person's home or where they

12 Judgment of 19 October 2016 in case C-582/14 (Patrick Breyer v Bundesrepublik Deutschland), point

41.

13 Same, point 43.

---

is located […] and on different legal and social relations associated with this name

(school/studies, medical records, bank accounts). […] All these new elements

information related to the name can allow someone to "zoom in" on the person

in the flesh, and thanks to the identifiers, the initial piece of information is then associated

to a natural person who can be distinguished from other persons”.14

40. In the present case, the Restricted Committee would like to point out that the electronic mail

of October 19, 2019 did not only contain the Claimant's surname, but

also her gender, her e-mail address containing a typing error, but allowing

to deduce the first letter of the claimant's first name, as well as detailed information

on three concrete pathologies from which the claimant suffers. Furthermore, the address

e-mail of the control employee who sent the disputed e-mail, as well as the

forms attached to said letter which contained the address of the life insurance company

concerned and in particular Luxembourg as the sending country are information which

may be associated with the complainant for the purpose of identifying him.

41. The same applies to e-mail sent

erroneously dated November 29, 2018. The last name of the

claimant, gender, e-mail address containing a typing error, but

allowing to deduce the first letter of his first name, very precise questions as to

to a specific pathology, the surname of the life insurance doctor and a

indication of his address, as well as two non-completed forms referencing the said

pathology.

42. The Restricted Committee therefore considers that, contrary to the claims of the

checked, the data transmitted by the two litigious e-mails allow

to identify the claimant, at least indirectly, and are therefore to be qualified as

personal data within the meaning of Article 4.1 of the GDPR.

2.2. As to the presence of a personal data breach

14 Opinion 4/2007 on the concept of personal data, adopted 20 June 2007, WP 136, p. 13 and 14.

43. The Restricted Committee notes first of all that the document […] of the controlled

of December 4, 2018 is very brief and does not contain any analysis on the qualification

data that was disclosed by the two disputed e-mails and on

their possible consequences for the data subject. She therefore cannot

accept the assertion of the controller contained in his letter of November 29, 201915 that

said document contained the essential information required by Article 33.5 of the GDPR,

especially since this [document] is dated almost seven weeks after the first

contentious letter.

44. Next, she wishes to recall that WP 250rev.01 (p.8) classifies breaches of

personal data according to three information security principles:

“breach of confidentiality” – the unauthorized or accidental disclosure or access to

personal data; “integrity breach” – unauthorized tampering

or accidental personal data; “availability violation” – the

accidental or unauthorized destruction or loss of access to personal data

personal character. »

45. Sending e-mails containing personal data

to an incorrect recipient is therefore to be qualified as a data breach

personnel of the “breach of confidentiality” type, the latter having led,

accidentally, disclosure of personal data to persons

third parties who were not authorized to take cognizance of the information contained

in e-mails and their attachments.

46. The Restricted Panel therefore finds that the two cumulative conditions

triggering the obligation provided for in Article 33.5 of the GDPR are met, that is to say that

personal data has been subject to a data breach

personal within the meaning of Articles 4.1 and 4.12 of the GDPR. Thus, that the violations must be

notified to the controlling authority or not, the controlled should have documented the violations

15 Original text: […]

Survey no. […] conducted with Company A.

in its internal personal data breach register as required

by article 33.5 of the GDPR.16

47. In view of the foregoing, she thus agrees with the finding of the head of investigation17 according to

which the auditee did not comply with its obligation to document these two breaches of

personal data and that it is therefore necessary to hold against him a non-

compliance with the requirements of article 33.5 of the GDPR.

B. On the breach of the obligation to notify a data breach to

personal character to the supervisory authority

1. On the principles

48. According to the provisions of Article 33.1 of the GDPR, the controller

is required to notify any personal data breach to the supervisory authority

“as soon as possible and, if possible, 72 hours at the latest after taking

knowledge, unless the violation in question is not likely to cause

a risk to the rights and freedoms of natural persons. »

49. According to recital (87) of the GDPR, it “should be checked whether all the

appropriate technical and organizational protective measures have been implemented

works to immediately establish whether a personal data breach

has occurred and to promptly inform the supervisory authority and the data subject.

It should be established that the notification was made as soon as possible, taking into account

particular of the nature and severity of the personal data breach

and its consequences and negative effects for the data subject. Such a

notification may lead a supervisory authority to intervene in accordance with its missions

and its powers set out in these regulations. »

50. In order to comply with Articles 33 and 34 of the GDPR, WP 250rev.01

recommends “both for controllers and processors of

have a documented notification procedure defining the procedure to be followed

16 See WP250rev.01, p.30

17 Statement of Objections, p. 5.

---

when a breach is detected, including how to contain, manage and

remedy the incident, assess the risk and notify the breach. In this regard, always in order

to prove their compliance with the GDPR, it could be useful to demonstrate that the

employees have been informed of the existence of such mechanisms and procedures and that they

know how to react in the event of a violation. »

51. WP250rev.01 (p.31) advises “that the controller document

also the reasoning behind the decisions taken in response to the breach. In

In particular, where a violation is not notified, the justification for this decision should

be documented. This justification should include the reasons why the

controller considers that the breach is unlikely to result in a

risk to the rights and freedoms of individuals. »

52. With regard specifically to the assessment of the risk to the rights and freedoms

of individuals presented by a personal data breach, the

WP250rev.01 (p.27) recommends that the data controller must take into account the

specific circumstances of the breach, including the seriousness of the consequences

potential events and the likelihood of them occurring. More specifically, he

recommends that the assessment take into account the following criteria: the type of violation, the

nature, sensitivity and volume of personal data, the ease

identification of the persons concerned, the seriousness of the consequences for the data subjects, the particular characteristics of the data subjects and of the controller, as well as the number of data subjects.18 In the event of doubt, the data controller should err on the side of caution and carry out a notice (WP250rev.01 (p.29).

2. In this case

53. In his Statement of Objections of 29 October 2019, the Head of Investigation retained that a “disclosure of sensitive data, providing information on several pathologies serious afflicting the plaintiff, risks in particular causing the latter damage material or moral, such as discrimination, financial loss or damage

18 For more details, see pages 27 to 30 of WP250rev.01.

economic and social significance if, for example, such information would be published or would be transmitted to other third parties, or even to his employer. Note also that it is also a loss of data which was protected both by medical secrecy only by insurance secrecy and that the controller, company insurance company is bound by a reinforced obligation to respect confidentiality in view of very sensitive data that it is required to process". He concluded that the control was under the obligation to notify this breach of personal data to the CNPD and that therefore it is necessary to hold against him a non-compliance with the provisions of article 33.1 GDPR. (Statement of Objections, p.5)

54. In its letter of response to the statement of objections of 29 November 2019, the auditee referred to his previous letters, emphasizing again that,

as he felt that the information disclosed by the two e-mails does not

would not qualify as personal data and that therefore, no violation

such data would not have taken place, it follows logically that he did not notify this

incident at the CNPD.

55. The Restricted Panel would like to point out that Article 33.1 clearly indicates

that a violation which is “not likely to create a risk for the rights and freedoms

natural persons” does not have to be notified to the supervisory authority, but must

only be documented in the internal data breach register.

56. One of the key factors in risk assessment is the type and character

sensitive personal data that has been compromised by the breach.

According to WP250rev.01 (p. 27), “the more sensitive the data, the greater the risk of

damage will be high for the persons concerned […]. »

57. In the present case, it should be taken into account that the data disclosed to

unauthorized persons fell under special categories of data, and more

specifically health data19 of the claimant, of a nature

particularly "sensitive" with regard to his private life. Processing of such

19 See the definition of data concerning health provided for in article 4.15 of the GDPR: “personal data

personnel relating to the physical or mental health of a natural person, including the provision of

health care services, which reveal information about that person's health status. »

---

special categories of personal data is even specifically

governed by article 9 of the GDPR.

58. While in general, the larger the number of people involved, the more

the potential consequences of a violation are numerous, the Restricted Formation also agrees with WP250rev.01 (p. 29) that a “breach may, however, also have serious consequences for even one person depending on the nature of the personal data and the context in which it was compromised. Furthermore, even if it is only a limited amount of data to be personal character implied by the breach, due to the highly sensitive nature of said data, the potential damages for the claimant are particularly serious, because the violation could lead to material or moral damages, such as discrimination, financial loss or economic and social harm material if, for example, such information would be published or transmitted to other third parties, even to his employer.20

59. With regard to the “security” aspect, developed in more detail under point "D. On the breach of the obligation to guarantee the security of the processing of personal data”, it is important to emphasize that “if the data to be personal character have been rendered incomprehensible to any unauthorized third party and if the data in question constitute a copy or that there is a backup, a breach of confidentiality relating to personal data correctly encrypted does not need to be notified to the supervisory authority. The reason is that such violation is unlikely to result in a risk to the rights and freedoms of physical persons. (WP250rev01, p.21). However, the Restricted Panel finds that the two litigious letters were not protected at all by techniques guaranteeing a effective protection according to the current state of the art, such as encryption by encryption or the use of strong and separately shared passwords, especially since particularly sensitive information was contained in the e-mails litigious.

20 See also WP250rev.01, p.28.

60. Even “when a violation is not notified, the justification for this decision should be documented. This justification should include the reasons why the controller considers that the breach is unlikely to result in a risk to the rights and freedoms of individuals. (WP250rev.01 (p.31). Training Restricted nevertheless notes that the document […] of the inspection of December 4, 2018 is not very detailed and above all does not contain any explanation why the auditee considered that the violation did not create a risk for the rights and freedoms of the claimant and that therefore, no notification would have been necessary.

61. It should also be noted that the “nature and role of the controller as well as of its activities may affect the level of risk that a breach creates for the persons concerned. (WP250rev.01 (p.29). Considering that the controlled is a insurance company […] - life and that the personal data disclosed were both protected by the medical secrecy provided for by article 458 of the Luxembourg Penal Code, only by the professional secrecy of the insurance companies in accordance with article 300 of the law of December 7, 2015 on the insurance sector, the control was held at a reinforced obligation to respect confidentiality in view of the very sensitive data that it is brought to deal with.

62. The EDPS advises in this context in his Guidelines 01/2021 on examples of data breach notifications of January 14, 2021 only if an email was sent to an unauthorized/wrong recipient, the controller will have to send an additional letter to said recipient requesting that the disputed mail be deleted.21 The Restricted Panel has

nevertheless of no documentation which would prove that the controlled person asked the

unauthorized recipients, i.e. the owners of the addresses […] to delete

disputed emails. During the hearing of the Restricted Panel on 14

July 2021, the control clarified that the owners of the aforementioned addresses have not

not responded to the two litigious letters, but that the employee who sent the said

couriers did not have a response that the above addresses did not exist

21 Original text, paragraph 117: “If an email is sent to an incorrect/unauthorized recipient, it is

recommended that the data controller should Bcc a follow up email to the unintended recipients apologising,

instructing that the offending email should be deleted, and advising recipients that they do not have the right

to further use the email addresses identified to them. »

---

not. Therefore, without any information on the recipients of the two letters

electronic, they cannot be considered as "reliable", i.e. as

a recipient towards whom the controlled would have had a certain degree of confidence "of

in such a way that it can reasonably be expected that the latter will not read the data

sent by mistake or does not access them and that he satisfies his request to send them to him

send back. ". 22

63. In view of all these elements, the Restricted Panel concludes that the two

personal data breaches in question were likely to result in

a risk for the rights and freedoms of the claimant and that therefore, the controlled should have

notify the CNPD. It is therefore necessary to hold against him a non-compliance with the

prescribed by article 33.1 of the GDPR.

C. On the breach of the obligation to communicate to the data subject

a personal data breach

1. On the principles

64. Article 34 of the GDPR provides the following:

“1. Where a personal data breach is likely

create a high risk for the rights and freedoms of a natural person, the

controller communicates the data breach

personnel to the data subject as soon as possible.

2. The communication to the data subject referred to in paragraph 1 of this

article describes, in clear and simple terms, the nature of the data breach at

personal character and contains at least the information and measures referred to in

Article 33(3)(b), (c) and (d).

3. The communication to the data subject referred to in paragraph 1 is not

required if either of the following conditions is met:

22 See WP250rev.01 (p.29).

a) the controller has implemented the protective measures

appropriate technical and organizational measures and these measures have been applied to

personal data affected by said breach, in particular the

measures which render the personal data incomprehensible to

anyone who is not authorized to access it, such as encryption;

b) the controller has taken subsequent measures which ensure that

the high risk to the rights and freedoms of data subjects referred to in

paragraph 1 is no longer likely to materialize;

(c) it would require disproportionate effort. In this case, it is rather carried out a

public communication or a similar measure enabling persons

concerned to be informed in an equally effective manner.

4. If the data controller has not already communicated to the person

concerned the breach of personal data concerning him, the authority of

control may, after examining whether this data breach of a nature

personnel is likely to create a high risk, require the person in charge of the

treatment that it carries out this communication or decide that one or other of the

conditions referred to in paragraph 3 are fulfilled. »

65. Recital (86) of the GDPR specifies that the "… communication should

describe the nature of the personal data breach and formulate

recommendations to the natural person concerned to mitigate the negative effects

potentials. Such communications to data subjects should be

carried out as quickly as reasonably possible […]. »

2. In this case

66. In his Statement of Objections of 29 October 2019 (p.6), the Head of Investigation

considered that then "even if it is established in this case that the controller has

actually contacted the complainant twice, it cannot be argued that the

obligations of Article 34 have nevertheless been complied with. Indeed, apart from the fact that the

person in charge admits not to be in the presence of a data breach of character

personnel, the conditions of paragraph (2) of the said article have not been complied with in the

communication with the data subject. He was so of opinion

that the auditee was under an obligation to communicate a data breach to

personal nature to the claimant, given that this breach presented a risk

high for the rights and freedoms of the data subject and that he has failed to do so. For

For this reason, the head of investigation found against the person inspected a non-compliance with the

prescribed by Article 34.1 of the GDPR.

67. In its letter of response to the statement of objections of 29 November

2019, the audited explained that, as he believed that the information disclosed by

the two e-mails would not qualify as personal data

personal and that therefore no breach of such data would have taken place, he also did not

no longer communicated the violation to the complainant under the conditions of Article 34 of the GDPR.

On the other hand, he considered that he had always been transparent towards the Claimant by informing him

incidents and that their CEO and DPO have explained the case to them in more detail.

68. The Restricted Committee wishes to emphasize in this context that it is only

when a violation is likely to create a “high” risk for the rights and

freedoms of natural persons that they must also be informed by

the controller. The threshold to be reached is therefore higher for the

communication to data subjects only for notification to the supervisory authority.

While the notion of "high risk" is not defined by the GDPR, WP250rev.01

(p.26) specifies that such a high risk “exists when a violation is likely

to cause physical or material damage or moral harm to the

individuals whose data has been breached. Examples of such

damages are discrimination, theft or impersonation, financial loss or

damage to reputation. Where the breach involves […] data concerning the

health or data concerning sex life or data relating to

criminal convictions and offences, or security measures

related, such damage is considered likely to occur. » 23

69. Referring to the arguments developed in points 55 to 63 of this

decision, the Restricted Committee considers that the personal data involved

by the violations are very sensitive data concerning the complainant's health which

23 See also recitals (75) and (85) of the GDPR.

could lead to material or moral damages, such as discrimination,

significant financial loss or economic and social damage if, for example,

this information would be published or transmitted to other third parties, or even to its

employer. It is therefore of the opinion that the two violations presented a high risk

for the rights and freedoms of the claimant and that the controlled was under the obligation to

communicate them to him within the meaning of article 34.1 of the GDPR. According to paragraph 2

of that article, the controller should at least provide the information

following:

~ a description of the nature of the violation;

~ the name and contact details of the data protection officer or other

point-of-contact ;

~ a description of the likely consequences of the violation;

~ a description of the measures taken or that the controller proposes

to take to remedy the breach, including, where appropriate, measures

to mitigate any negative consequences.

70. In this case, the Restricted Panel finds that on November 7, 2018, almost

three weeks after the first disputed email of October 19, 2019 was sent,

the claimant was informed by the control by email that unfortunately an address

erroneous has been used and that it is only as of this day that this error has been

discovery. As regards the second disputed letter of 29 November 2018, the

claimant was informed by email of December 3, 2018 which specified that shipments

repetitive errors have occurred and the insurance DPO has been notified. It was indicated there

also that all measures will be taken to avoid such incidents in the future.

In addition, the CEO of the audited proposed to the complainant by email of February 27, 2019

a telephone conversation to discuss the incidents. The DPD sent him by

elsewhere an additional email dated March 26, 2019 by which he

explained to the claimant that the controller considered that, even if the data sent

incorrectly by the two e-mails would have been read by a third party,

they would not qualify as personal data, and that therefore it has not

treated the incidents as data breaches.

71. Even if the Restricted Committee considers that certain information from the

complaint has taken place, it nevertheless considers that the requirements of Article 34.1 of the GDPR

have not been complied with and that the communications to the controller do not contain the

information provided for in paragraph 2 of that article.

72. In view of the foregoing, the Restricted Panel concludes that Article 34.1 of the

GDPR has not been respected by the controller.

D. On the breach of the obligation to guarantee the security of the processing of personal data

1. On the principles

73. According to Article 5.1.f) of the GDPR, personal data must be "processed in a way that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against the loss, accidental destruction or damage, using technical measures or appropriate organizational (integrity and confidentiality). »

74. Considering the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, including the degree of likelihood and severity varies, for the rights and freedoms of individuals physical, the controller is bound under paragraph (1) of Article 32 of the GDPR to "implement the technical and organizational measures appropriate to guarantee a level of security appropriate to the risk, including between others, as needed:

a) pseudonymization and encryption of personal data;

b) the means to guarantee the confidentiality, integrity, availability and the ongoing resilience of processing systems and services; […]"

2. In this case

75. In his letter of August 8, 2019, the inspector explained to the head of investigation his communication process with its customers. He explained that communication by electronic means is done either by using an electronic portal […] or by mail electronic. In the latter case, the controller would contact the client to ask for his consent as to the possibility of sending e-mails containing

---

sensitive medical data by email and where consent is given, staff should
keep sensitive content to a minimum. In addition, the controller also specified in
said mail only attachments to e-mails and containing
Sensitive information would be protected by separately shared passwords.

76. The auditee returned to the issue of data protection in the event of
of sending emails in a letter dated September 17, 2019, where he explained
that the security measures detailed in its aforementioned letter of August 8, 2019 do not
only concern documents containing sensitive information. As
the questionnaires sent to the Claimant were empty, they did not contain, according to the
controlled, no such information and in addition, as no person related to these
questionnaires was not identifiable, protection was not necessary. The aforementioned letter
of September 17, 2019 also contains in annex the document […] and which indicates that
henceforth all e-mails would be sent from a common mailbox,
that all PDF files would be password protected and names would be
replaced by initials.

77. According to the head of investigation, the information contained in the letters
electronic
disputed had, on the other hand, a sensitive nature and were not
"manifestly not adequately protected so as not to be able to be
accessed or read by incorrect email recipients. In view of the character
particularly sensitive information contained in e-mails
litigious, encryption by encryption or any technique guaranteeing protection
similar would, according to the current state of the art and good practices applicable in the

matter, had to be applied to the communications in this case in order to ensure a level of security adapted to the risks of invasion of the privacy of the data subject. » (Statement of Objections, p.7). He concludes that the controlled party did not respect his obligation to guarantee the security of the processing of personal data and that it failure to hold against him a non-compliance with the prescriptions of articles 5.1.f) and 32.1. a) and b) GDPR.

78. In its letter of response to the statement of objections of 29 November 2019, the controller recalled that, following erroneous shipments, security measures additional measures have been put in place to avoid such incidents in the future. They are referred again to the [document] of December 4, 2018, reiterating that henceforth all

e-mails would be sent from a common mailbox, which all PDF files would be password protected and names would be replaced with initials.

79. The Restricted Committee notes first of all that the form […] sent by the controlled by letter of September 17, 201924 contains on its page […] the sentence following: “I authorize […] to send emails containing sensitive medical information to the email address indicated below" with two checkboxes ("Yes" and "No"), the box “Yes” was checked, and a line […] on which the claimant had indicated his mail address […].

80. Nevertheless, without analyzing whether the consent given corresponds to the requirements valid consent within the meaning of Article 4.11 of the GDPR, the signature of such clause in no way exempts the auditee from its obligations resulting from Articles 5.1.f) and 32.1.

a) and b) of the GDPR mentioned above. Protecting the privacy and security of

personal data is an even more important issue in the event of

processing of sensitive data (health data) insofar as the disclosure of

this data could cause serious harm to the customers of the controlled […].

81. The Restricted Committee also notes that Article 34.3 of the GDPR provides in

this context that the communication to the data subject of a data breach

is not necessary if "the controller has implemented the measures of

appropriate technical and organizational safeguards and these measures have been applied

to the personal data affected by the said breach, in particular the

measures which render the personal data incomprehensible to any

person who is not authorized to access it, such as encryption". For instance,

in the event of a breach of the confidentiality of personal data which has been

encrypted using a state-of-the-art algorithm and that the confidentiality of the encryption key

is intact, the data is in principle incomprehensible and the violation is therefore not

likely to harm the persons concerned and would not need their

communicated.25 In addition, WP250 rev.01 contains concrete examples in

24 See appendix 3 of the audit letter of 17 September 2019.

25 WP250 rev01. p. 21

which notification of a breach to the supervisory authority is or is not mandatory,

depending on the security measures in place, such as means of encryption

secure or hashed and salted passwords in secure mode.26

82. These considerations bear witness to the importance that the legislator has given

European Union, like the EDPS, to the security measures which may, where appropriate, to prevent a violation or, in the event of its occurrence, to mitigate the risks for the rights and freedoms of natural persons.

83. Considering that in the present case, the disputed emails of October 19 2018 and of 29 November 2018 did not only contain attached forms separate forms to be completed relating to the claimant's pathologies which have been declared to his insurance, but also included in the body of the text indications and questions very detailed as to the very specific pathologies affecting the Claimant, the Restricted Training considers that undoubtedly sensitive data relating to the Claimant's health were disclosed by said letters.

84. As a result, ciphering by encryption, passwords or any technique guaranteeing similar protection according to the current state of the art and best practices applicable in the matter, should have been applied to the communications in this case in order to guarantee a level of security adapted to the risks of invasion of the privacy of the person concerned, especially for a company like that of the auditee. However, as the sending of the two disputed e-mails was not protected by any technical measure making it possible in particular to guarantee the confidentiality of messages and documents transmitted, the Restricted Panel considers that the control did not comply with its security obligations provided for in Articles 5.1.f) and 32.1. a) and b) GDPR. Whether such security measures would have been in place from the outset, breaches of personal data could even have been avoided, or at least their consequences could have been mitigated.

85. In view of the foregoing, the Restricted Panel concludes that Articles 5.1.f) and 32.1. a) and b) of the GDPR have not been complied with by the auditee.

26 See for details WP250 rev01. p. 20 to 22.

E. On the failure to communicate the contact details of the
data protection officer at the supervisory authority

1. On the principles

86. Pursuant to Article 31.1 of the GDPR, the controller and the processor
processing must appoint a DPO 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
into processing operations which, due to their nature, scope and/or
their purposes, require regular and systematic monitoring on a large scale of
persons concerned; Where
(c) the core activities of the controller or processor consist of
in large-scale processing of special categories of data referred to in
Article 9 or personal data relating to convictions
criminal offenses and offenses referred to in Article 10.”

87. Article 37.7 of the GDPR provides in this context that “the data controller
processing or the processor publish the contact details of the data protection officer
data and communicate them to the supervisory authority. »

88. The obligations in this area have been clarified by the Article
29 in its Guidelines for Data Protection Officers (DPOs)
the revised version of which was adopted on 5 April 2017. It should be noted that the EDPS has taken over and
reapproved the documents adopted by the said Group between May 25, 2016 and May 25,
2018, as precisely the aforementioned guidelines on the DPO.27

2. In this case

27 See EDPS Endorsement Decision 1/2018 of 25 May 2018, available

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

_____

under :

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

Survey no. […] conducted with Company A.

89. During the on-site visit of 29 July 2019, it was stated to the agents of the

CNPD that […] was absent during the on-site investigation, was designated as DPO. However,

the CNPD officials noted that the appointment of the latter was not subject to

a notification to the CNPD as provided for in article 37.7 of the GDPR and that no

no explanation for this omission has been provided.28

90. By letter dated July 23, 2019, the controller specified that the DPO was abroad

during the on-site visit by CNPD officials and affirmed that […] was designated DPD

of the company in early 2018.

91. In the Statement of Objections of 29 October 2019, the Head of Investigation

nevertheless considered that the contact details of the DPO designated by the controller were not

communicated in good and due form to the CNPD and that the information on the

designation of the DPO in the audit letter of July 23, 2019 "is not likely to

irritate this observation, while neither the minimum information to be transmitted, nor the procedure

provided for by the CNPD have not been respected. »

92. In its letter of response to the statement of objections of 29 November

2019, the control reiterated that the contact details of the DPD were revealed to the agents of the

CNPD during their on-site visit and in its letter of July 23, 2019. It noted by

other than Article 37.7 of the GDPR only requires that the contact details of the DPO are

communicated to the supervisory authority, without imposing any particular formalism on respect. For the communication of the coordinates of the new DPO, the control indicated have used the form provided by the CNPD.

93. The Restricted Committee considers in this context that the form made available provision on the CNPD website and allowing the contact details of the DPO to be transmitted to the CNPD is only intended to facilitate this process for data controllers / subcontractors, while avoiding having to request information possibly missing. On the other hand, the communication of the contact details of the DPO by another means of communication, for example by post, is quite

28 See finding 1 of minutes no. […]/2019 relating to the on-site fact-finding mission carried out on July 19, 2019 with Company A.

acceptable, provided that the necessary information, as detailed in said form, are included.

94. Nevertheless, it notes that at the time of the on-site visit by the agents of the CNPD dated July 29, 2019, that is to say more than a year after the entry into force application of the GDPR, the contact details of the DPO of the controller had not been communicated, by any means whatsoever, to the CNPD.

95. In view of the foregoing, the Restricted Panel concludes that at the time of the on-site visit by CNPD agents, article 37.7 of the GDPR was not respected by Control.

II. 2. On corrective measures and fines

1. Principles

96. In accordance with article 12 of the law of 1 August 2018, the CNPD has the

power to adopt all the corrective measures 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

these regulations;

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 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, paragraph 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. »

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

98. Article 83 of the GDPR provides that each supervisory authority shall ensure that the administrative fines imposed are, in each case, effective, proportionate and deterrents, before specifying the elements that must be taken into account to decide whether 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 pursuant to

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 to what extent 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".

99. The Restricted Committee wishes to specify that the facts taken into account in the

context of 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.

100. Nevertheless, the steps taken by the control to put itself in

compliance with the GDPR during the investigation process or to remedy the
shortcomings noted by the head of investigation in the statement of objections, are taken
taken into account by the Restricted Training in the context of any corrective measures
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

101. In its supplementary letter to the statement of objections of 15
December 2020, the head of investigation proposed to the Restricted Panel to impose a
administrative fine to the control of an amount of 275,000 euros.

102. In its response to said additional letter of January 27, 2021, the audited
considered that on the basis of the criteria provided for in Article 83.2 of the GDPR, the amount proposed
by the head of investigation was disproportionate. In particular, he argued that the alleged
violation concerned only one person by sending only two letters
erroneous electronic messages, that the violation would not have lasted over time and that the person
concerned would not have suffered any damage. Furthermore, the alleged violation was not
that the result of regrettable human error, but would not have been intentional and not
related to the lack of supervision by the controller in terms of data protection.

103. In order to decide whether to impose an administrative fine and to
decide, where applicable, the amount of this fine, the Restricted Panel takes into
includes the elements provided for in Article 83.2 of the GDPR:

~

As to the nature and seriousness of the breach (Article 83.2.a) of the GDPR), the
Restricted Panel notes that with regard to the breach of Article 5.1.f)
of the GDPR, it constitutes a breach of the fundamental principles of the
GDPR (and data protection law in general), namely the principle
of integrity and confidentiality set out in Chapter II “Principles” of the GDPR.

As for the failure to have put in place the technical measures and
appropriate organizational measures to guarantee a level of security adapted to the
risk, in accordance with Article 32.1 of the GDPR, the Restricted Training considers
only in the face of the risks represented by data breaches
personnel, the European legislator has intended to strengthen the obligations of
data controllers with regard to the security of processing. Thus, according to the
recital (83) of the GDPR and in order to "guarantee the security and prevent any
processing carried out in violation of this Regulation, it is important that the
controller or processor assesses the risks inherent in the
treatment and implements measures to mitigate them, such as
encryption. These measures should ensure an appropriate level of security, including
including confidentiality, taking into account the state of knowledge and the costs of
implementation in relation to the risks and the nature of the personal data
personnel to be protected. […] . However, considering that the two e-mails
disputed have not been protected by techniques guaranteeing protection
effective according to the current state of the art, such as encryption by encryption or
the use of strong passwords, especially since information
particularly sensitive were contained in the e-mails
contentious, the Restricted Panel considers that the person audited did not measure correctly
value the importance of securing the personal data contained in
its systems.

Considering, moreover, that the controlled person is an actor […] in the sector of

life insurance with […] employees in Luxembourg29 and […]30 and that the data of a personal nature disclosed were both protected by medical secrecy provided for by article 458 of the Luxembourg Penal Code, only by secrecy insurance professional in accordance with article 300 of the amended law of 7 December 2015 on the insurance sector, the control was held at a reinforced obligation to respect confidentiality in view of the very data sensitive that it is brought to treat.

29 See […]

30 See […]

As to the failure to document the data breaches at personal nature internally and not having notified them to the CNPD, nor communicated to the data subject, the Restricted Panel observes that the said shortcomings had their origin in an erroneous interpretation, eyes of the head of investigation and the Restricted Training, of two basic notions of data protection, i.e. the notions of “personal data” personnel” and “personal data breaches” within the meaning of the articles 4 points 1) and 12) of the GDPR. However, as a life insurance company dealing large-scale sensitive data of its customers, the control should have had the necessary knowledge in the matter to be able to carry out a correct characterization of the facts.

~

As for the duration criterion (article 83.2.a) of the GDPR), the Restricted Training

finds that breaches of Articles 5.1.f), 32.1. a) and b), 33.1, 33.5 and 34.1
of the GDPR have lasted over time, at least since the first violation of the
data from October 19, 2019 and up to the day of the on-site visit, while the
violation of Article 37.7 of the GDPR lasted from May 25, 2018 until at least the day
of the on-site visit. The Restricted Formation recalls here that two years separated
the entry into force of the GDPR from its entry into force to allow
controllers to comply with their obligations.
Moreover, a comparable obligation to implement the measures
appropriate technical and organizational measures based on the risk of harm to the
privacy, as well as the state of the art and the costs related to their implementation existed
already in application of articles 22 and 23 of the repealed law of August 2, 2002 relating
the protection of individuals with regard to the processing of personal data
personal.

~

As for the number of data subjects (Article 83.2.a) of the GDPR), the
Formation notes that in general, the more the number of people concerned is
higher, the greater the potential consequences of a violation. By
against, it considers that in the present case the violation may also have serious
consequences even for one person, i.e. the claimant,
due to the nature of the personal data and the context in

which they were compromised. Thus, due to the highly
sensitive of said data, the potential damages for the claimant are

particularly serious, as violation could result in property damage

or moral, such as discrimination, financial loss or damage

economic and social significance if, for example, such information would be

published or would be transmitted to other third parties, or even to his employer.

Furthermore, the Restricted Panel considers that as the shortcomings

observed are part of the daily practice of control and are consecutive

the lack of implementation of adequate security measures in the event of the sending of

sensitive data by e-mail, a large number of other people,

beyond the only

claimant, are potentially

impacted by

said

shortcomings. Indeed, as the data in question were not identified by the

controlled neither as personal data nor as sensitive data

(health data) within the meaning of Article 9 of the GDPR, there is a risk that many

other cases where customers have opted in to sending sensitive medical data

by e-mail and where the security measures were also insufficient,

were not detected by the controller.

The Restricted Committee is therefore of the opinion that

The number of people

potentially affected is high.

~

As to whether the breaches were committed deliberately

or not (by negligence) (article 83.2.b) of the GDPR), the Restricted Panel reminds

that “not deliberately” means that there was no intention to commit the

breach, although the controller or processor has not

complied with the duty of care incumbent upon it under the 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 of the controlled. On the other hand, given that very personal data sensitive were sent twice to unauthorized third parties, some negligence is to be remembered.

~

As for the measures taken by the auditee to mitigate the damage suffered by the data subjects (article 83.2.c) of the GDPR), the Restricted Training takes account of the measures taken by the auditee and refers to Chapter II.2. section 2.2. of this decision for the related explanations.

~

As for the degree of responsibility of the controller, taking into account the technical and organizational measures that it has implemented under the articles 25 and 32 (article 83.2.d) of the GDPR), the Restricted Training takes account that the two litigious letters were not protected by techniques guaranteeing effective protection according to the current state of the art, such as a encryption by encryption or the use of passwords, especially since particularly sensitive information was contained in the letters disputed electronics.

~

As for the categories of personal data concerned by the

violation (Article 83.2.g) of the GDPR), it should be taken into account that the
data disclosed to unauthorized persons fell into the categories
particular data, and while it was more specifically the data
claimant's health, of a particularly "sensitive" nature to the
regard to his private life.

~

As to how the supervisory authority became aware of the breach,
in particular if, and to what extent, the controller or the data processor
processor has notified the breach (Article 83.2.h) of the GDPR), the Restricted Panel shall
to be referred to paragraphs 55 to 63 of this Decision where it arrived at the
conclusion that the controller should have notified the violations to the CNPD, but did not
not done. Thus, the violation came to the attention of the CNPD by
the lodging of a complaint by the data subject.

104. The Restricted Committee notes that the other criteria of Article 83.2 of the
GDPR are neither relevant nor likely to influence its decision on the taxation
an administrative fine and its amount.

---

105. Regarding the breach of the obligation to notify data breaches
to the CNPD, pursuant to Article 33.1 of the GDPR, the Restricted Panel considers
that this failure is basically linked to an erroneous legal interpretation of the
events by the controlled. Indeed, as he considered that the information disclosed
by the two e-mails would not be qualified as personal data
personal and that therefore no violation of such data would have taken place, it follows in

his logic that he did not need to notify these incidents to the CNPD either. She
therefore considers that, in view of the circumstances of the case, there is no reason to sit
its fine on the basis of this breach, although it is characterized.
106. With regard to the failure to communicate violations of
data to the data subject, pursuant to Article 34.1 of the GDPR, the Training
Restricted considers that partial information of the claimant took place, on the one hand, and that
this breach is also fundamentally linked to an erroneous legal interpretation of the
events by the controlled, on the other hand. Indeed, as he considered that the information
disclosed by the two e-mails would not qualify as data to
personal character and that therefore no violation of such data would have taken place, it is
follows in its logic that there was also no need to communicate these incidents to the
data subject in accordance with Article 34.1 of the GDPR. She therefore considers
that in view of the circumstances of the case, there is no reason to base its fine on the
basis of this failure, although it is characterized.
107. With regard to the failure to communicate the contact details of
contact with the supervisory authority, pursuant to Article 37.7 of the GDPR, the Training
Restricted considers that the essential obligation is to have designated by May 25, 2018
a DPO in the event of application of one of the three conditions provided for in Article 37.1 of the GDPR.
Indeed, the DPO occupies a fundamental place within the legal framework created by the
GDPR. It therefore considers, as the auditee had designated a DPO at the beginning of 2018, but
had only omitted to communicate his contact details to the CNPD, that there is no need
to base its fine on the basis of this breach, although it is characterized.
108. The Restricted Committee also notes that while several measures have been
put in place by the auditee in order to remedy in whole or in part certain shortcomings,
these were only adopted following the inspection by CNPD officials on
19 July 2019 (see also point 99 of this decision).

109. Consequently, the Restricted Committee considers that the imposition of a fine administrative is justified with regard to the criteria laid down by article 83.2 of the GDPR for breach of Articles 5.1.f), 32.1. a) and b) and 33.5 GDPR.

110. With regard to the amount of the administrative fine, the Restricted Panel recalls that paragraph 3 of Article 83 of the GDPR provides that in the event of breaches multiple, as is the case here, the total amount of the fine cannot exceed the amount fixed for the most serious violation. To the extent that a breach of article 5 of the RGPD is reproached to the controlled, the maximum amount of the fine being able to to be retained amounts to 20 million euros or 4% of the worldwide annual turnover, the the highest amount being retained.

111. With regard to the relevant criteria of Article 83.2 of the GDPR mentioned above and taking into consideration the size of the controlled and information about its finances […] the Restricted Committee considers that the pronouncement of a fine of one hundred and thirty-five thousand euros (135,000 euros) appears to be both effective, proportionate and dissuasive, in accordance the requirements of Article 83.1 of the GDPR.

2.2. About taking corrective action

112. The adoption of the following corrective measures, which should be implemented within three months, under penalty of penalties of 750 euros per day of delay, was proposed by the head of investigation to the Restricted Training in its additional letter to the statement of objections of December 15, 2020:

“(a) Order the controller to document any breach of personal data, for example by means of a "register of

violations";

b) Order the data controller to notify any data breach to

personal nature to the CNPD, unless the violation in question is not

likely to create a risk for the rights and freedoms of individuals

physical;

c) Order the controller to notify, as soon as possible, any

breach of personal data to the data subject when the

---

violation is likely to result in a high risk to the rights and freedoms of a

Physical person ;

d) Order the controller to implement measures

appropriate technical and organizational measures to guarantee a level of security

adapted to the risk, including the encryption of personal data

covered by Article 9 of the GDPR, in order to guarantee their confidentiality;

e) Order the controller to publish the contact details of the delegate to

designated data protection officer and communicate them to the CNPD. »

113. In its response to said additional letter of January 27, 2021, the audited

referred to his letter of November 29, 2019 in which he had taken a position with regard to

to all the shortcomings mentioned in the Statement of Objections. Furthermore, he has

mentioned that all corrective measures proposed by the head of investigation would be

already implemented. Thus, each data breach would be recorded in […] including

the incidents in question, and would be notified to the CNPD (unless there is no risk for

the rights and freedoms of data subjects) and to the data subject (unless he

there is no high risk to the rights and freedoms of data subjects). By

elsewhere, security measures would be put in place and the contact details of the DPO have

been published on their website and communicated to the CNPD by letter dated October 11, 2019.

114. As for the corrective measures proposed by the head of investigation and by

reference to point 100 of this decision, the Restricted Training takes into account

the steps taken by the control, following the visit of the CNPD agents, in order to

comply with the provisions of articles 5.1.f), 32.1. a) and b), 33.1, 33.5, 34.1 and 37.7 of

GDPR, as detailed in his letters of July 23, 2019, August 8, 2019, 17

September 2019, November 29, 2019, and January 29, 2021. More

in particular, it takes note of the following facts:

~

As for the obligation to internally document any data breach to

personal nature, to notify them, if necessary, to the CNPD, and to

communicate, where appropriate, to the persons concerned, the Restricted Training

notes that from now on, the audited registers each data breach in a […]

including the incidents in question, notifies them to the CNPD (unless there is no

risk to the rights and freedoms of data subjects) and to the person

concerned (unless there is no high risk for the rights and freedoms of

persons concerned).

Furthermore, the Restricted Committee notes that since the first notification

of a data breach received by the controlled on October 11, 2019, a

twenty data breaches were notified to the CNPD.

In consideration of the compliance measures taken by the control in

case and point 100 of this decision, the Restricted Panel considers

since there is no reason to pronounce the corrective measures proposed by

the head of investigation and repeated under a), b) and c) of point 112 above.

~

As for

the obligation to implement measures

techniques and

appropriate organizational measures to guarantee a level of security adapted to the

risk, including the encryption of personal data relating to

article 9 of the GDPR, in order to guarantee their confidentiality, the control indicated that

security measures would have been put in place, such as sending

e-mails from a common mailbox, protection of the sending of

PDF files by passwords, replacing names with initials and

encryption of personal data referred to in Article 9 of the GDPR.

However, the Restricted Training does not have the documentation

to demonstrate the implementation of these compliance measures

by the controlled. It therefore considers that it is appropriate to pronounce the measure

correction proposed by the head of investigation and repeated under d) of point 112 above.

~

Regarding the obligation to publish the contact details of the designated DPO and to

communicate to the CNPD, the Restricted Panel finds that the contact details

of the DPD have been published on the site of the control and communicated to the CNPD by

a statement received on October 17, 2019.

In consideration of the compliance measures taken by the control in

case and point 100 of this decision, the Restricted Panel considers

since there is no reason to pronounce the corrective measure proposed by the

head of investigation and repeat under e) of point 112 above.

The Restricted Committee also considers that there is no need to impose a

obligation to the controlled to compel him to comply with these corrective measures.

In view of the foregoing developments, the National Commission sitting

in restricted formation and deliberating unanimously decides:

- to retain the breaches of articles 5.1.f), 32.1. a) and b), 33.1, 33.5, 34.1 and 37.7 of

GDPR;

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

one hundred and thirty-five thousand euros (135,000 euros) with regard to breaches of the

articles 5.1.f), 32.1. a) and b) and 33.5 GDPR;

- issue against Company A an injunction to bring the

treatment with Articles 5.1.f) and 32.1. a) and b) GDPR within two months

following notification of the Restricted Committee's decision, in particular:

- protect the sending of e-mails containing special categories of

data within the meaning of Article 9 of the GDPR by appropriate security measures, such as

encryption by encryption, strong passwords and shared separately or by

any other technique guaranteeing similar protection according to the current state of the art and

best practices in this area.

Thus decided in Belvaux on August 5, 2021.

For the National Data Protection Commission sitting in formation

restraint

Tine A. Larsen

Thierry Lallemang

Christopher Buschman

President

Commissioner

Commissioner

Indication of remedies

This administrative decision may be the subject of an appeal for review in the

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

and must be introduced through a lawyer at the Court of one of the Orders of

lawyers.
