Decision of the National Commission sitting in restricted formation

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

Deliberation No. 11FR/2021 of April 8, 2021

The National Commission for Data Protection sitting in restricted formation

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

Lemmer, commissioners;

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

During its deliberation session on February 14, 2019, the National Commission for

data protection sitting in plenary formation (hereafter: “Plenary Formation

”) had decided to open an investigation with the ABC1 group on the basis of Article 37 of the

law of 1 August 2018 on the organization of the National Commission for the protection

data and the general data protection regime (hereinafter "Law of 1 August

2018”) and to appoint Mr. Christophe Buschmann as head of investigation.

According to the decision of the Plenary Formation, the investigation carried out by the

National Commission for Data Protection (hereinafter: “CNPD”) had as its

purpose of verifying compliance with the provisions of the regulations relating to the protection of

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

free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”)

and the law of August 1, 2018, in particular by setting up systems for

video surveillance and geolocation, where applicable, installed by the three companies in the

ABC group.

On February 20, 2019, CNPD agents visited the

premises of the ABC group. Since Minutes no. […] relating to the said mission

of the on-site investigation only mentions, among the three companies of the ABC group, as

controller controlled the company "Company A" 2, the decision of the Commission

national body for data protection sitting in restricted formation on the outcome of

the investigation (hereinafter: “Restricted Training”) will be limited to controlled processing

by CNPD officials and carried out by the company “Company A”.

"Company A", is a […] registered in the Trade and Companies Register of

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

1 And more specifically with companies: Company A, registered in the Trade and

Luxembourg companies under number […], with registered office at L-[…]; Company B, listed on

Luxembourg Trade and Companies Register under number […], with registered office at L-

[…] and Company C, registered in the Luxembourg Trade and Companies Register under number

[…], with registered office at L-[…] .

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

of February 20, 2019 with the company Company A.

---

is in the business of providing consultancy, installation and

maintenance in technology […] .3

During the aforementioned visit of February 20, 2019 by CNPD agents to the

controlled premises, Mr. X, Director of Human Resources for the controlled,

confirmed to CNPD officials that a geolocation device is installed in a

part of the vehicles in the controlled vehicle fleet, but that the latter does not use

a CCTV system.4

According to the explanations provided to CNPD officials, the persons concerned

by geolocation are company employees who use the vehicles for their

trips to customers and on their professional journey between their home and the head office

social of the controlled. Mr. X also confirmed to CNPD officials that each

vehicle is allocated to a specific employee and that part of the vehicles which can be

used by employees for private purposes is not equipped with a device for

geolocation.5

At the end of his investigation, the head of investigation had the person inspected notified on 9

August 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 article 13 of the GDPR with regard to employees, non-compliance with the

measures prescribed by Article 32.1 of the GDPR, as well as non-compliance with the requirements

prescribed by Article 5.1.e) of the GDPR.

The request for a meeting by the control of August 13, 2019 was accepted by the head

of investigation and the meeting took place on August 20, 2019.6

3 According to the information provided on its own website: […] .

4 See Minutes no. […] relating to the on-site fact-finding mission carried out on 20 February

2019 with company Company A; see also the email from Company A of March 1, 2019 and

the mail of March 29, 2019.

5 See finding 1 of minutes no. […] relating to the on-site fact-finding mission carried out on

of February 20, 2019 with the company Company A.

6 See minutes of the meeting of August 20, 2019 with Company A.

On October 7, 2019, the auditee produced written observations on the

statement of objections.

An additional letter to the statement of objections was sent to the controller

dated August 17, 2020. In this letter, the head of investigation proposed to the Panel

Restricted from taking three different corrective actions, as well as inflicting on the controlled

an administrative fine of EUR 4,000.

By letter dated September 24, 2020, the controller produced written observations

on the supplementary letter to the statement of objections.

The president of the Restricted Formation informed the control by mail of the 9

October 2020 that his case would be registered for the session of the Restricted Panel on 17

November 2020. The controller confirmed his presence at the said meeting dated October 20

2020.

During the Restricted Training session of November 17, 2020, the head

investigation and control reiterated their written observations orally and responded to the

questions asked by the Restricted Panel. The controller spoke last.

II. Place

II. 1. As to the reasons for the decision

A. On the breach linked to the principle of limitation of storage

1. On the principles

In accordance with Article 5.1.e) of the GDPR, personal data

must be kept "in a form which permits the identification of the persons

concerned for a period not exceeding that necessary with regard to the purposes

for which they are processed […]".

According to recital (39) of the GDPR “personal data should

be adequate, relevant and limited to what is necessary for the purposes for which

which they are processed. This requires, in particular, ensuring that the duration of

retention of data is kept to a strict minimum. Character data

personal should only be processed if the purpose of the processing cannot be

reasonably achieved by other means. In order to ensure that the data is not

not kept longer than necessary, time limits should be set by the

controller for erasure or for periodic review […]. »

2. In this case

During the on-site investigation, it was explained to CNPD officials that the purposes

of geolocation are as follows: “geographic tracking, protection of

company assets, tracking of goods transported, optimal fleet management,

the optimization of the work process, the provision of answers to the complaints of the

customers, the provision of proof of services, the invoicing of services as well as the

tracking the working time of employees on the move".7

With regard to the retention period of data from the device of

geolocation, it appears from the findings of CNPD agents that the oldest

data dated from October 14, 2016, i.e. the retention period of the

data was 2 years and 4 months.8

According to the head of the investigation, the said retention period for the data of

geolocation of 2 years and 4 months exceeded that which was necessary to carry out the

aforementioned purposes and for which the geolocation system had been implemented.

square. For this reason, he was of the opinion that a non-compliance with the requirements of Article 5.1.e)

of the GDPR is to be retained (see statement of objections, Ad.A.3).

7 See finding 5 of minutes no. […] relating to the on-site fact-finding mission carried out on

of February 20, 2019 with the company Company A.

8 See finding 4 of minutes no. […] relating to the on-site fact-finding mission carried out on

of February 20, 2019 with the company Company A.

By letter dated March 29, 2019, the controller for his part reiterated the comments contained

in its email of March 1, 2019, specifying that the retention period

data from the "[…]" geolocation system had been adapted to 12 months,

limit that was already in place for the "historical" pane but not yet for the pane

"general reports".9

During the hearing of the Restricted Panel on November 17, 2020, the controlled

clarified that the retention period of 12 months was justified, among other things, by the fact that

location data is used for billing customers for services

carried out by its employees.

The Restricted Training recalls that it is up to the data controller to

determine, according to each specific purpose, a retention period

appropriate and necessary to achieve that purpose. Thus, as the system of

geolocation set up by the control has several purposes, the durations of

conservation are to be individualized for each specific purpose.

The Restricted Panel considers that the control should have differentiated

between the retention period of location data for the purpose of

geographical tracking, tracking of transported goods and optimal management of its fleet,

on the one hand, and the data relating to the working time of employees having precisely

for the purpose of monitoring the working time of employees on the move, on the other hand.

As mentioned above, during the hearing of the Restricted Panel, the subjugated

further specified that the geolocation data also have the purpose of invoicing

customers of the services provided by its employees. As a result, the Restricted Formation

believes that an appropriate retention period should have been determined in order to achieve

the said purpose.

With regard to the geolocation of employee vehicles, the Training

Restricted considers that

personal data obtained by

the

geolocation can in principle only be kept for a period

maximum of two months under the aforementioned principle of Article 5.1.e) of the GDPR.

9 Regarding the different functionalities of "[...]", see the explanations of the controlled in

his letter of October 7, 2019.

However, it considers that if said data is used by the person responsible for the processing for the purposes of proof for the invoicing of the services carried out for its customers, the data necessary for such invoicing may be kept for a duration of one year, provided that it is not possible to provide proof of the services by other means.10

In case the geolocation device is installed for verification of the working time (when this is the only possible means), the Restricted Training considers that the personal data obtained by the geolocation which allow to check the working time may nevertheless be kept for a period maximum of three years in accordance with the limitation period set out in article 2277 paragraph 1st of the Civil Code in matters of action for payment of employee compensation.

In the event of an incident, the Restricted Panel is of the opinion that the data may however, be kept beyond the time limits mentioned in the context of the transmission of the data to the competent judicial authorities and to the authorities law enforcement authorities competent to establish or prosecute criminal offences.

It also wishes to point out that the data obtained by geolocation may also be kept beyond the aforementioned durations, if these have been previously made anonymous, i.e. it is no longer possible to make a link – direct or indirect – between this data and a specific employee.

In its former authorization No […], on which the control is based, among other things to justify that the employees were already informed of the implementation of the system of

geolocation, the CNPD had already imposed as a condition that the data of

geolocation could not be kept for more than two months, respectively three

years for working time data.

Based on all of these elements, the Restricted Panel concludes that

Article 5.1.e) of the GDPR has not been complied with by the auditee.

10 See in this context the article by the Commission Nationale de l'Informatique et des Libertés

(CNIL): "The geolocation of employee vehicles", available at: https://www.cnil.fr/fr/la-

geolocation-of-employee-vehicles. »

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

1. On the principles

Under the terms of paragraph 1 of Article 12 of the GDPR, the "controller

take appropriate measures 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 the treatment to the data subject in a concise manner,

transparent, understandable easily accessible, in clear and simple terms […]. »

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

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

obtained, the following additional information which is necessary to guarantee

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. »

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 obligations transparency within the meaning of the GDPR.11 These obligations have been explained by the Article 29 Working Party in its guidelines on transparency within the meaning of Regulation (EU) 2016/679, the revised version of which was adopted on 11 April 2018 (here after: “WP 260 rev.01”).

It should be noted that the European Data Protection Board (hereinafter: "EDPS), which has replaced the Article 29 Working Group since May 25, 2018, took over and reapproved the documents adopted by the said Group between May 25, 2016 and May 25, 2018, such as the aforementioned guidelines on transparency12.

2. In this case

According to the head of the investigation, the employees of the control were not validly informed on the specific elements of Article 13.1 and 2 of the GDPR (see statement of objections, page 2, Ad.A.1.).

11 See in particular Articles 5,1,a) and 12 of the GDPR, see also recital (39) of the GDPR.

12 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.

By letter dated March 29, 2019, the controller for his part reiterated the comments contained in his email of March 1, 2019 stating that already before the visit to CNPD site, a plastic sheet was added to the on-board vehicle documents equipped with a geolocation system specifying that the vehicle is equipped with such a system, on the one hand, and that said vehicles had a label on the rear door informing the driver of the presence of said system, on the other hand.

The controller attached to the aforementioned letter of March 29, 2019 a statement from the staff delegation dated March 27, 2019 and certifying that it was informed of the installation of a geolocation system in certain vehicles of the ABC group.

By letter dated October 7, 2019, the inspector also sent the head of the investigation a copy of the information note intended for all staff on the system of geolocation and which has been displayed since October 4, 2019 on the controlled site, as well as than a photo of its display.

Finally, in his letter of September 24, 2020, the controller added that in […], an authorization for geolocation had been issued by the CNPD13 and that already at that time, the employees had been informed of the implementation of the system of geolocation, in particular via staff delegation. The controller specified that he asked the staff delegations of the ABC group to kindly attest to the fact that information to staff was actually provided in 2009.

The Restricted Training first of all wishes to point out that Article 13 of the GDPR makes reference to the obligation imposed on the data controller to “provide” all the information mentioned therein. The word "provide" is crucial here and it "means that the data controller must take concrete measures to provide the information in question to the person concerned or to actively direct the person concerned to the location of said information (for example by means of a link direct, a QR code, etc.). (WP260 rev. 01. paragraph 33).

13 See deliberation no. […].

The statement by the staff delegations of Company A and Company B of the

March 27, 2019 certifies in this context that they were informed of the establishment of a geolocation system in some ABC group vehicles, while the joint certificate of September 14, 2020 of the said delegations indicates that they were "duly informed by the controller of the implementation of a system of geolocation in company vehicles. It should be noted that the delegations of the staff have been informed since it was set up in 2009. […]. »

However, the Restricted Panel considers that a simple declaration, respectively a certificate by the delegation of control staff indicating that they have been informed of the presence of the geolocation device does not ensure that the employees of the company have been duly informed in accordance with article 13.1 and 2 of the GDPR, especially since the said documents are dated after the on-site visit by the agents of the CNPD.

Furthermore, as mentioned above, the controlled party indicates in its statement of 24 September 2020 that, as he had an authorization from the CNPD of […], the employees had already been informed at that time of the implementation of the geolocation, in particular via staff delegation.

The only possible derogation from the information obligations referred to in Article 13 of GDPR of a data controller is indeed "when, and insofar as, the data subject already has this information. The principle of responsibility however, requires data controllers to demonstrate (by documenting) what information was already in the possession of the data subject, how and when it has received it and no changes have been made to this information likely to render them obsolete.15

The Restricted Panel notes, however, that no documentation submitted by the audit does not contain proof that the information of the employees has indeed taken place

14 According to Article 13.4 of the GDPR.

15 See WP260 rev. 01, paragraph 56.

---

in 2009, at least in relation to the requirements provided for by the legislation in force in
the time16.

Next, the Restricted Panel would like to point out that there is in the GDPR a
“inherent conflict between, on the one hand, the requirement to communicate to data subjects
the complete information that is required under the GDPR and, on the other hand, the requirement
to do so in a concise, transparent, understandable and easily accessible manner. »
(WP260 rev. 01, para. 34) Prioritize the information to be provided to people
involved and determine what levels of detail and methods are appropriate for the
communication of information is not always easy.

It is for this reason that a multi-level approach to communicating information
transparency information to data subjects may be used in a
offline or non-digital context, i.e. in a real environment such as
for example personal data processed through a system of
geolocation. The first level of information should generally include the
most important information, namely details of the purpose of the processing, the identity
of the controller and the existence of the rights of data subjects, as well as
that the information having the greatest impact on the processing or any processing
likely to surprise those concerned. The second level of information
i.e. the other information required under Article 13 of the GDPR, could
be provided later and by other means, such as a copy

of the privacy policy sent by e-mail.17

Finally, the joint certificate of the staff delegations of the companies

Company A and Company B of September 14, 2020 indicates that the said delegations have to

were again informed when the information note on the system of

geolocation intended for all staff on October 4, 2019. The part

annexed to the observations of the audit of September 24, 2020 contains the said note

information and a photo of its display.

16 In accordance with article 26 of the repealed law of 2 August 2002 on the protection of

individuals with regard to the processing of personal data.

17 See WP260 rev. 01 (item 38).

The Restricted Panel notes, however, that the plastic sheet added to the

vehicle documents indicating only that the vehicle "is equipped with a

geolocation”, as well as the label affixed to the rear door of the vehicle

mentioning “Monitored by GPS with […]”18 do not even respect the requirements of the

mandatory content of the first level of information. Added to this is that the control failed

to its obligation to put in place a confidentiality policy which contains all the

information required in accordance with Article 13.1 and 13.2 of the GDPR.

In view of the foregoing, the Restricted Panel concludes that Article 13 of the GDPR

was not respected by the controller.

C. On the breach of the obligation to guarantee appropriate security

1. On the principles

Under Article 32.1 of the GDPR and "taking into account the state of knowledge,

the costs of implementation and the nature, scope, context and purposes of the

treatment as well as risks, the degree of likelihood and severity of which vary, for the

rights and freedoms of natural persons, the controller and the processor

implement the appropriate technical and organizational measures in order to

guarantee a level of security appropriate to the risk including, among other things, as required:

a) pseudonymization and encryption of personal data;

b) the means to guarantee the confidentiality, integrity, availability and

ongoing resilience of processing systems and services;

c) means to restore the availability of personal data

and access to them in a timely manner in the event of a physical or technical incident;

(d) a procedure for regularly testing, analyzing and evaluating the effectiveness of

technical and organizational measures to ensure the security of the processing. »

18 There is also a link to the website of the developer of said software … .

---

2. In this case

The head of investigation examined the aspect related to the security of access to data

listed in the geolocation system. As access to the operating software of the

geolocation device was only secured by means of an identification

unique, i.e. a unique user name and password, which is used by

all persons authorized to access said software, he held against the controlled

non-compliance with the measures prescribed by

GDPR Article 32.1 (see

statement of objections, Ad.A.2).

The auditee defends himself based on his written observations of October 7, 2019

relating to the email he sent in this context on August 21, 2019 to the

person who manages access to users' accounts of the geolocation system.

In said letter, the controller asks the person who manages access to accounts

users to create personalized logins and passwords for

people who have access to “[…]”19 and to delete existing logins, on the one hand, and

ensure that passwords are regularly updated and not communicated to

third parties, on the other hand. In addition, it is specified that the "perimeter to which they have access

remains unchanged (so only the vans of the service for which these people

working) ".

The Restricted Panel finds that on the day of the visit by CNPD agents

in the premises of the controlled, the access policies to the geolocation software do not

did not meet the minimum necessary requirements in terms of safety, i.e.

have individual accounts in place using a username and password

for persons authorized to access it as part of the performance of their

assignments.

In view of the foregoing, the Restricted Panel concludes that Article 32.1 of the GDPR

was not respected by the controller.

19 This is the name of the geolocation software developed by […].

II. 2. On corrective measures and fines

1. Principles

In accordance with article 12 of the law of August 1, 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 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, 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. »

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

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".

The Restricted Panel would like to point out 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.

Nevertheless, the steps taken by the control to bring itself into compliance

with the GDPR during the investigation process or to remedy breaches

noted by the head of investigation in the statement of objections, are taken into account by

Restricted Training as part of any corrective measures to be taken

and/or setting the amount of any administrative fine.

2. In this case

2.1. Regarding the imposition of an administrative fine

In its supplementary letter to the statement of objections of August 17, 2020,
the head of investigation proposed to the Restricted Panel to impose an administrative fine
to the audit relating to the amount of 4,000 euros taking into account the elements
following:

~ "The fact that clear and complete information for the persons concerned about the
processing(s) implemented by the controller constitutes a
an essential condition for these data subjects to be able to know
the existence of said processing, but also to understand its extent. Do not provide these
information or providing it incomplete will not only prevent
data subjects to understand what will happen to their data
personal character, but will effectively deprive them of exercising all the rights of
remedies granted to them by the GDPR.

~ The fact that partial information of the persons concerned has actually been
carried out.

~ The scale of the geolocation system, installed in at least 191 vehicles.

~ The good cooperation of the company throughout the investigation as well as its willingness

to comply with the law as soon as possible. »

In its response to said additional letter of September 24, 2020, the controller argued in particular that the concrete criteria taken into account by the head of the investigation led to the determination of the quantum were unclear and he did not understand on what objective elements the proposal for the fine would have been made.

In order to decide whether to impose an administrative fine and to decide, the where applicable, the amount of this fine, the Restricted Panel analyzes the criteria posed by 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.e) of the GDPR, it constitutes a breach of one of the fundamental principles of the GDPR (and data protection law in general), namely the principle the limitation of the retention of data set out in Chapter II “Principles of the GDPR.

~

As regards the breach of the obligation to inform persons in accordance with Article 13 of the GDPR, the Restricted Training recalls that the information and the transparency relating to the processing of personal data are essential obligations incumbent on data controllers so that data people are fully aware of the use that will be made of their personal data, once collected. A failure to

Article 13 of the GDPR thus constitutes an infringement of the rights of individuals concerned. This right to information has also been reinforced under the terms of the GDPR, which demonstrates their particular importance.

~

As for the duration criterion (article 83.2.a) of the GDPR), the Restricted Training notes that these shortcomings have persisted over time, at least since the May 25, 2018. 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 and this even if a comparable information obligation existed pursuant to Article 26 of the repealed law of August 2, 2002 on the protection of persons with regard to the processing of personal data.

With regard to the retention period of the data, the Restricted Training would like to point out that already in its authorization n° […], the CNPD had imposed provided that the personal data cannot be kept for more than two months, respectively three years for the data relating to working time.

~

As regards the number of data subjects (Article 83.2.a) of the GDPR), such as the checked specified that each vehicle is allocated to a specific employee, the number of people concerned corresponds to the number of vehicles fitted with a geolocation system.

During the hearing of the Restricted Panel on November 17, 2020, the person audited confirmed that the “ABC” group has a total of 191 vehicles equipped with a geolocation system, as also retained by the head of the investigation in his supplementary letter to the statement of objections of 17 August 2020.
Nevertheless, he clarified that the company "Company A" only has 92 vehicles equipped with a geolocation system.
As the head of investigation limited the scope of the investigation to one of the three companies of the "ABC" group and more specifically to the company "Company A", the Formation Restricted retains only 92 vehicles, unlike the 191 vehicles mentioned by the head of investigation, corresponding to 92 people who are affected by the processing implemented by the geolocation system.

~

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.

~

As for the degree of cooperation established with the supervisory authority (Article 83.2.f) of the GDPR), the Restricted Training takes into account the assertion of the head of investigation that the co-operation of the auditee throughout the investigation was good, as well as than its desire to comply with the law as soon as possible.

As to the mitigating circumstances applicable to the circumstances in this case (article 83.2.k) of the GDPR), the Restricted Training takes into account the elements following:

o partial information of the persons concerned has been carried out, in particular by the plastic sheet added to the on-board documents indicating that the vehicle “is equipped with a geolocation system”, as well as the label affixed to the rear door of the vehicle stating " Monitored by GPS with […]”;

oh taking measures to comply with Articles 12 and 13 of the GDPR, in particular through the development and display on its site of a note information on the geolocation system intended for the entire personal ;

oh the reduction of the retention periods of the data contained in the geolocation system from 2 years and 4 months to 12 months.

The Restricted Panel notes that the other criteria of Article 83.2 of the GDPR are neither relevant nor likely to influence its decision on the imposition of a administrative fine and its amount.

With regard to the breach of the obligation to ensure data security, in application of Article 32 of the GDPR, the Restricted Panel considers that, in view of the measures taken by the company, in particular the efforts undertaken to create logins and

personalized passwords for people who have access to "[...]" and

delete existing logins and ensure that passwords are regularly

updated and not communicated to third parties, it has acted in good faith within the framework

of the procedure. Consequently, the Restricted Committee considers that, with regard to the

circumstances of the case, there is no need to base its fine on the basis of this

failure, although it is characterized.

The Restricted Committee also notes that while several measures have been implemented

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

February 20, 2019.

Therefore, the Restricted Committee considers that the imposition of a fine

administrative is justified with regard to the criteria laid down by article 83.2 of the GDPR for

breach of Articles 5 and 13 of the GDPR.

Regarding 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 multiple violations,

as is the case here, the total amount of the fine cannot exceed the amount

set for the most serious violation. To the extent that a breach of Articles 5 and

13 of the GDPR is blamed for the controlled, the maximum amount of the fine that can be

retained amounts to 20 million euros or 4% of worldwide annual turnover, the amount

the highest is retained.

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

Restricted Formation considers that the pronouncement of a fine of 2,800 euros appears

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

2.2. About taking corrective action

The adoption of the following corrective measures has been proposed by the head of investigation to the Restricted Training in its additional letter to the communication of the grievances:

“a) Order the data controller to put in place information measures intended for persons concerned by geolocation, in accordance with the provisions of Article 13, paragraphs (1) and (2) of the GDPR by informing in particular the identity and contact details of the controller, where applicable, the contact details of the data protection officer, the purposes of the processing and its basis

legal, the categories of data processed, the legitimate interests pursued by the controlled, the recipients, the retention period of the data as well as the rights of the person concerned and how to exercise them, and the right to introduce a complaint to a supervisory authority;

b) Order the data controller to take any security measures in the context of the use of the operating software of the geolocation device, in particular (i) to define authorizations to access the geolocation operating software at the only people for whom it is strictly necessary for the performance of their missions and (ii) to create individual accounts by means of an identifier and a password for the persons authorized above;

c) Order the controller to implement a retention period policy.

retention of personal data in accordance with the provisions of e) of

Article 5 of the GDPR, not exceeding the duration necessary for the purposes for which they

are collected, and in particular by not keeping location data for more than

two months and data relating to working time for a maximum of

three years. »

As for the implementation of a retention period policy for data at

personal character in accordance with the provisions of Article 5.2.e) of the GDPR, the controller has

adapted after the on-site visit by CNPD officials the retention period of the

data from the geolocation system from 2 years and 4 months to 12 months.

The Restricted Panel considers, however, that the retention periods of the

data from the geolocation system must be adapted according to the

different purposes pursued.

As for information intended for persons concerned by geolocation,

in accordance with the provisions of article 13.1 and 13.2 of the GDPR, the controller claims to have

developed and posted since October 4, 2019 on its website an information note on the

geolocation system for all staff.

The Restricted Committee considers, however, that the information note does not include

not all of the rights of data subjects under the terms of the

GDPR. Thus, the right to object (Article 21 of the GDPR) is not mentioned. Otherwise,

the information on the retention period of the data must be updated.

As for the obligation to put in place policies for access to the software of

geolocation pursuant to Article 32.1 of the GDPR, the Restricted Panel considers that

despite the efforts made by the controller, the latter must, by virtue of the principle of

“accountability” implementing mechanisms and procedures

internal procedures to demonstrate compliance with Article 32.1 of the GDPR.

In view of the foregoing developments, the National Commission sitting

in restricted formation and deliberating unanimously decides:

- to pronounce against the company Company A an administrative fine of one

amount of two thousand and eight hundred euros (2,800 euros), with regard to the breaches

constituted in Articles 5.1.e) and 13 of the GDPR;

- to pronounce against the company Company A an injunction to bring it into compliance

processing with the provisions of Articles 5.1.e), 13 and 32.1 of the GDPR, within a period

two months following the notification of the Restricted Committee's decision, the supporting documents

compliance to be sent to the Restricted Training, at the latest,

within this period;

and especially :

1. with respect to the failure to implement a term policy

retention of personal data in accordance with the provisions of Article

5.1.e) of the GDPR: adapt the retention periods for personal data

obtained by geolocation according to the different purposes pursued, and

in particular by not keeping the personal data obtained by the

geolocation beyond two months, the personal data obtained by the

geolocation used for proof purposes for the invoicing of the services performed

for customers beyond one year and personal data obtained by the

geolocation which makes it possible to check the working time beyond three years;

2. as regards the breach of the obligation to inform the data subjects of the processing of their personal data in accordance with Article 13 of the GDPR: inform data subjects in a clear and complete manner, in accordance with the provisions of Article 13 of the GDPR, in particular by providing information relating to the duration of retention of data according to the purposes pursued and to all the rights some people ;

3. in respect of the failure to take any appropriate security measures in the context of the use of the operating software of the geolocation device under Article 32 of the GDPR, create individual accounts by means of an identifier and a password password only for people for whom access to the security system geolocation is strictly necessary for the accomplishment of their missions.

Thus decided in Belvaux on April 8, 2021.

For the National Data Protection Commission sitting in formation restraint

Tine A. Larsen Thierry Lallemang

Marc Lemmer

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.

_____