Decision no. MED-2025 -047 of 10 April 2025 issuing an order to

(N° MDM251019)

The vice-chair of the Commission nationale de l'informatique et des libertés (French Data Protection Authority),

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data (hereinafter the "GDPR");

Having regard to Act No. 78-17 of January 6, 1978, as amended, on data processing, data files and individual liberties, and in particular Article 20 (hereinafter referred to as the "Data Protection Act");

Considering decree No. 2019-536 of May 29, 2019 taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to deliberation No. 2013-175 of July 4, 2013 adopting the internal regulations of the Commission nationale de l'informatique et des libertés (French Data Protection Authority);

In view of decision No. 2023-006C of January 25, 2023 of the vice-chair of the French Data Protection Authority to instruct the Secretary General to carry out, or instruct others to carry out, verification of the data processing implemented by ;

In view of on-site inspection reports No. 2023-006/1 and 2023-006/2 dated January 26 and 27, 2023;

In view of online inspection report No. 2023-006/3 dated September 8, 2022;

Having regard to the other documents in the file;

I. The procedure

(hereinafter referred to as "the company" or "") is a public limited company with its registered office located at . It is one of the subsidiaries of the American company .

At December 31, 2022, the company had 759 employees. In 2023, it generated net banking income of over euros, with net income of euros.

issues and markets deferred debit payment cards for individuals and companies, enabling them to pay for goods and services at merchants

affiliated to the [redacted] network, in return for an annual fee. At the end of each month, the cardholder has the sum of the debits from the said card deducted from a bank account opened by him/her with a third-party bank, as [redacted] does not offer a bank account management service.

Several types of cards are available, with various associated services, including a range of insurance and assistance whose coverage and amount vary according to the card held.

In addition, the company offers its customers the possibility of taking out supplementary insurance (travel insurance, day-to-day insurance, provident insurance, legal protection). It acts as an intermediary between the insurer and the customer.

The company markets its products through its website [redacted] and distributes them through third-party banks. As the only subsidiary of the [redacted] group established in France as a payment institution, it has specified that its products are aimed at the French market, while other group entities are responsible for distributing [redacted] products in other European Union countries.

At December 31, 2022, the company had 836 879 customers in the European Union (for a total of 945 442 cards issued, as a single customer may hold several cards), including 831 443 residing in France (for a total of 939 416 cards issued).

The Commission nationale de l'informatique et des libertés's (hereinafter "the CNIL" or "the Commission") attention was drawn to the processing operations carried out by [redacted].

Thus, pursuant to decision No. 2023-006C of January 25, 2023 of the vice-chair of the CNIL, a delegation from the Commission carried out an on-site inspection at the headquarters of [redacted] on January 26 and 27, 2023.

The purpose of this investigation was to verify the company's compliance with the provisions of Law No. 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties (hereinafter "the Data Protection Act" or "Law of January 6, 1978 as amended") and Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter "the Regulation" or "GDPR").

The company was served with reports No. 2023-006/1 and 2023-006/2 on January 30, 2023, at the end of the investigation.

Pursuant to the same decision, an online inspection was carried out on January 30, 2023, via the [redacted] website. The resulting report was sent to the company on February 6, 2023.

The company provided the delegation with additional information on February 7, 14 and 21, April 7, May 16, June 23 and July 3, 2023.

On 10th May 2025, as part of the cooperation procedure, a draft decision was submitted to the supervisory authorities concerned on the basis of Article 60 of the GDPR.

This project did not give rise to relevant and reasoned objections.

II. The processing involved and the responsibility of [redacted]

In law, under Article 4(7) of the GDPR, the controller is *"the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing"*.

In this case, the processing operations at issue in the present proceedings are, on the one hand, those relating to the personal data of [redacted] employees and customers (holders of one or more payment cards issued by [redacted], and on the other hand those relating to the data of users of the web site [redacted]

Firstly, [redacted] provides its customers with several services accessible by telephone and, in this context, records certain calls. ACEF clearly identifies the means and purposes of this processing, which concerns the recording of telephone conversations between its employees and its customers, and which is intended, according to the company, to ensure the training of its employees, the verification of compliance and, more rarely (according to information provided by the company) the replay of calls in the event of a complaint.

In this respect, the company has requested the opinion of the CNIL, in 2015 and then in 2021, notably with regard to these recordings. During these exchanges, the content of which was communicated to the delegation by the company, the latter assumed the role of data controller**.**

Secondly, the company publishes the [redacted] website, from which it markets its products and enables its customers to manage their accounts. The pages of the site dedicated to legal notices, data protection and cookies designate [redacted] as the data controller.

In the light of all these elements, it must be considered that [redacted] is acting as the data controller for the processing of personal data on its behalf, concerning its employees, its customers and the users of its website.

III. Breaches of the GDPR

A. On the breach of the obligation of transparency and information to individuals (Articles 12 and 13 of the GDPR).

In law, Article 12(1) of the GDPR states that "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means."*

Under the terms of Article 13 of the GDPR, the data controller must provide the data subject, at the time of collection of his or her data, with various information relating in particular to his or her identity and contact details, the purposes of the processing implemented, its legal basis, the recipients or categories of recipients of the data as well as the fact that the data controller intends to transfer data to a third country. In addition, to guarantee "*fair and transparent processing*" of personal data, the regulations require that data subjects be informed of the time during which the data will be kept, the existence of the various rights available to individuals, the right to withdraw consent at any time, and the right to lodge a complaint with a supervisory authority.

With particular regard to informing the data subject of the purposes of the processing, it is recalled that Article 6 of the GDPR provides that processing is lawful only if, and insofar as, at least one of the legal bases listed in paragraphs a) to f) can be retained, and in particular if b) "*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*" or if f) "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal*".

With regard to informing individuals of their right to object, it should be recalled that Article 21(1) of the GDPR states that "*the data subject shall have the right to on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1)*".

In this case, the company indicated that calls made by agents in the "insurance" department were recorded in the event of the sale of an insurance policy. In this case, the agent concerned must manually trigger the recording ("on-demand recording") in order to specifically record the segment corresponding to the conclusion of the sale and the information that must be provided to the policyholder. The company has specified that these recordings are kept to establish proof

of the contract, which can be concluded orally by telephone in accordance with the provisions of article L.112-2-2 (V) of the French Insurance Code.

The sales script produced by the company reads as follows:

"Mrs X/Mr X, I am now going to record this part of the interview in order to validate the sale and keep proof of your agreement. If you have any questions regarding the recording of this call, I am at your disposal."

Should the individual request additional information, the hotliner must specify that:

"The data recorded may be listened to by authorized [redacted] *staff. They are necessary, excluding those indicated as optional. The recording of your conversation is kept for a maximum period of two months (except in the case of the purchase of an insurance product, in which case it will be kept for the duration of the applicable statute of limitations). In accordance with the French Data Protection Act, you have the right to access, rectify and object to the processing of your personal data, as well as the possibility of defining directives concerning the fate of your personal data in the event of your death with* [redacted] *by writing to the following address:* [redacted] *- délégué à la protection des données* [redacted]

In addition, call recordings provided to the delegation show that hotliners mention the following information: "*In accordance with the French Data Protection Act, I hereby inform you that the personal data collected during the recording is necessary for the issue and management of your contract. This data will be transmitted to insurer X. You have the right to access and rectify your information, which you may exercise by contacting X. You may also, for legitimate reasons, object to the processing of this data."*

Firstly, it should be noted that the legal basis for the processing is not clearly stated.

Indeed, as part of the call recordings provided to the delegation, the data subjects are told that the personal data collected during the recording is "*necessary for the issue and management [of] the contract*", thus basing the processing carried out on Article 6, paragraph 1, b) of the GDPR. However, a right to object is offered to data subjects, suggesting that the legal basis for processing would be the company's legitimate interest, and not the performance of a contract, as no right to object can be exercised in the context of processing based on this legal basis.

Thus, the information provided leaves room for doubt as to the legal basis enabling the company to collect and store data from call recordings. The information relating to the legal basis for the processing is therefore not delivered in a transparent, intelligible and easily accessible form or in clear and simple terms as required by Article 12 of the GDPR.

Secondly, it is clear from the above that the right to lodge a complaint with the CNIL is not mentioned.

Thus, the information provided to persons contacted by the "insurance" department when entering into a sale contract is incomplete and, moreover, is neither transparent nor intelligible. A breach of Articles 12 and 13 of the GDPR is therefore constituted.

It is the responsibility of [redacted] to provide complete, transparent and intelligible information to individuals contacted by the insurance department.

B. On the breach of the obligation to ensure data security and confidentiality (Article 32 of the GDPR).

In law, Article 32 of the GDPR requires the controller "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,[*to*] implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"* including "*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*". Where unpublished personal data is processed via a website, the controller is required to ensure the security of such processing.

In particular, it must use a secure protocol for data transmission between the user's browser and the server hosting the site. The "HTTP" protocol does not provide all the necessary security guarantees, unlike, for example, the "HTTPS" protocol. In particular, HTTP does not allow users to authenticate the site to which they are connected. In addition, the data transmitted by the browser to the server hosting the website is not encrypted.

Given the current state of the art, the ANSSI (French National Agency for the Security of Information Systems) has drawn up specific recommendations in its technical note on securing website communications, specifying in particular that the use of "*TLS, i.e. the use of the HTTPS protocol, is recommended whenever communications between the client and the server need to be protected in terms of confidentiality or integrity. This is particularly the case when transmitting identifiers, personal data, payment information, etc.*" (https://cyber.gouv.fr/sites/default/files/IMG/pdf/NP_Securite_Web_NoteTech.pdf).

The use of the "HTTP" protocol can therefore guarantee neither the confidentiality of the data exchanged (in the absence of encryption) nor the authentication of the website (in the absence of a certificate).

In this case, the online investigation carried out on the [redacted]/ website on January 30, 2023 revealed that, from the "*Become a customer*" tab at the top of the home page, a drop-down menu gave access to various sections, including "[redacted]". Within this section, a click on the button entitled "*Get more info*", positioned

in an insert on the right-hand side of the page, enabled the delegation to observe the opening, in a new tab, of a page with the URL [redacted] and on which appeared a contact form inviting users to provide personal information (title, surname, first name, e-mail address and optionally telephone number).

At the time of the findings on January 30, 2023, while the [redacted] website was indeed being navigated using the "HTTPS" protocol, this was not the case for the [redacted] page, to which the user was redirected. Indeed, this site did not implement any "HTTP" to "HTTPS" redirection. As a result, browsing and submission of the above-mentioned form was by default carried out using the "HTTP" protocol, which only allows the unencrypted transmission of data between people's terminals and the servers hosting the website. The information provided by users via the contact form could therefore be easily retrieved, modified or reused by an attacker.

Thus, by using the "HTTP" protocol, which can guarantee neither the confidentiality of the data exchanged nor the authentication of the website, the company didn't respect a basic security measure and exposed the personal data of its users to significant risks. Consequently, a breach of Article 32 of the GDPR appears characterized.

Nevertheless, during a subsequent informal verification, the delegation noted that this redirection was now being carried out correctly.

IV. Corrective measures ordered by the vice-chair of the CNIL (Article 20, paragraph III of the Data Protection Act)

As a result of the foregoing, [redacted] is subject to the following corrective measures:

- **A REPRIMAND**, in accordance with the provisions of Article 20, paragraph III of the French Data Protection Act *(Loi Informatique et Libertés*), with regard to the breach of the obligation to ensure the security and confidentiality of data under the provisions of Article 32 of the GDPR;
- **AN ORDER, within three (3) months of notification of this decision and subject to any measures it may already have taken, to** provide complete, transparent and intelligible information to people contacted by the insurance department.

This order and reprimand do not require any response from you to the CNIL. On the other hand, if subsequent investigations reveal the persistence or repetition of the breaches referred to in the order, I may appoint a rapporteur within the CNIL and refer the matter to the CNIL's restricted committee, or initiate proceedings under the simplified sanction procedure, without a new order being sent to you beforehand, so that one or more of the corrective measures provided for in Articles 20 et seq. of the amended Act of January 6, 1978 may be ordered.

The vice-chair

[redacted]