Decision no. MED 2020-041 on November 24, 2020, issuing formal notice to the company [redacted]

(N°MDM201040)

The Chair of the Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority),

Having regard to Treaty no. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

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 the free movement of such data, in particular articles 56 and 60;

Having regard to the French Postal and Electronic Communications Code;

Having regard to Act no. 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act), particularly its article 20;

Having regard to Decree no. 2019-536 of 29 May 2019, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the internal regulations of the Commission Nationale de l'Informatique et des Libertés;

Having regard to decision no. 2019-083C of 24 April 2019 of the Chair of the Commission Nationale de l'Informatique et des Libertés tasking the Secretary General with performing or assigning a third party to perform an investigation on the [redacted] and [redacted], subsidiaries of the [redacted];

Having regard to records of investigation nos. 2019-083/1 of 6 August 2019 and 2019-083/2 of 7 August 2019;

Having regard to the complaints no. 18007540, 18009275, 18021587, 18024134, 19000332, 19000605, 19001259, 19004708, 19006278, 19008043;

Having regard to the other items in the case file;

I. The procedure

The single-shareholder simplified joint-stock company [redacted] (hereinafter "the company"), a subsidiary of the [redacted], operates as an affinity insurance broker, mainly for telephone and multimedia products. It has approximately 800 employees. Its registered office is located at [redacted].

During 2018 and 2019, the Commission was referred to regarding several complaints made by customers and prospects stating that the company had not complied with their rights to access, object to and erase their personal data.

Pursuant to the Chair of the Commission nationale de l'informatique et des libertés' (hereinafter the "CNIL") decision no. 2019-083C, a CNIL delegation conducted two on-site investigations on 6 and 7 August 2019 regarding the [redacted], with a view to verifying the compliance of the personal data processing carried out by the latter.

In this context, the company informed the delegation that it conducts telephone and email marketing campaigns to sell its insurance policies using prospect lists purchased from its partners, which are mainly companies specialised in the collection and sale of prospects' data and companies distributing telephone or multimedia products. To date, around two million individuals are said to be concerned by the company's marketing activities.

The company subsequently provided the delegation, by email, with additional documents requested as part of the investigation relating, in particular, to the number of prospect personal data files purchased by the company, copies of marketing emails sent by the company, the methods used to verify the validity of prospects' consent to receiving marketing emails collected by the company's partners.

On September 22, 2020, a draft decision was submitted to the concerned supervisory authorities as part of the cooperation procedure, on the basis of Article 60 of the GDPR.

This draft decision did not give rise to relevant and reasoned objections.

II. The breaches

A breach of the requirement to obtain the consent of a data subject targeted by a direct marketing operation via email

Pursuant to Article L. 34-5 of the Postal and Electronic Communications Code, "*direct marketing through automatic calling machines, facsimile machines (fax) or electronic mail that use the contact details of a natural person who has not given prior consent to receiving direct marketing through said media is prohibited*". The same article also provides that "*consent shall be understood as any free, specific and informed indication of the data subject's wishes by which he/she accepts that his/her personal data be used for marketing purposes*".

Furthermore, Article 4. 11) of the Regulation defines consent as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

Lastly, Article 7.2. of the Regulation provides that "*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language*". As a result, the data subject should be able in theory to give their consent independently and specifically for each distinct purpose.

The delegation was informed and found that the company conducted email marketing campaigns to sell its insurance products using prospect lists purchased from its different partners.

The company informed the delegation that its partners are contractually required to provide it with prospect lists containing the data of individuals having consented to their data being transferred to partners. Data subjects' consent is therefore collected by the provider of the prospect list.

However, the delegation found that partner companies [redacted], [redacted], [redacted] and [redacted] collect data subjects' consent using only one box to be ticked on a consent form relating to at least two separate processing of personal data: participation in a competition and consent to receiving marketing messages from partners.

Therefore, data subjects' consent to the use of their data for marketing purposes by the contracting third parties is not collected in accordance with applicable provisions.

Thus, even though the company does not collect itself data prospects' consent, the company could not conduct marketing campaigns targeting data subjects appearing in the prospect list bought from partner companies [redacted], [redacted], [redacted] and [redacted], since then the data subjects 'consent had not been validly collected.

By conducting marketing campaigns targeting data subjects whose consent to receive marketing messages had not been validly collected, the company acted in breach of the provisions of Article L. 34-5 of the Postal and Electronic Communications Code and of Articles 4 and 7 of the Regulation.

A breach of the requirement to provide proof that consent was given by the data subject

Article 7.1. of the Regulation provides that "*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his/her personal data*".

The delegation found that the company's partners are responsible for collecting data subjects' consent to the processing of their personal data for marketing purposes.

The delegation was also informed and found that, when a prospect disputes that their consent has been collected, a request is sent to the provider of the file to ensure consent has indeed been given and an audit of the process to collect consent is conducted by the partner.

The company was therefore able to provide the delegation with documents, such as the consent collection forms presented by partner companies to their customers, enabling to establish, in general, the process implemented by its partners to collect prospects' consent. The delegation was further informed that a tool had been introduced in 2018 to track the origin of prospect lists. This tool provides the origin of each prospect and provides the prospect with information when requested.

However, the delegation found that the verification process implemented by the company in respect of its partners does not enable it to ensure that consent has indeed been given individually by each of the prospects.

Thus, the company is not able to prove that each of the individuals targeted by its marketing campaign have indeed given their consent to the processing of their data.

These actions are in breach of article 7.1 of the GRPD.

A breach of the requirement to inform data subjects

Article 13 of the GDPR requires that, at the time when data are obtained, the data controller provides information relating to its identity and contact details, the contact details of the data protection officer, the purposes of the processing and its legal basis, the recipients of the personal data, where applicable the transfer of personal data, the period of storage of the data, the rights of data subjects and the right to lodge a complaint with a supervisory authority.

However, the delegation was informed and found that, when recording telephone conversations, the script followed by telesales personnel does not provide for the complete information of prospects. By listening to a sample of telephone conversations held, the delegation noted that, while the individuals contacted are indeed informed of the principle of recording, they are not, however, informed of the rights that they possess, and in particular of their right to object to the recording of their telephone conversation.

These actions are in breach of the requirement to inform data subjects pursuant to Article 13 of the GDPR.

A breach of the requirement to keep a complete record of processing activities

Article 30 of the Regulation provides that a data controller enterprise employing fewer than 250 persons is required to hold a record of processing activities when its personal data processing is not occasional.

In this case, the record of processing activities must contain all information listed under Article 30.1 of the GDPR, i.e.: the name and contact details of the controller, its representative and the data protection officer, the purposes of the processing, the categories of data subjects and the categories of personal data, where applicable the transfers of data and where possible the envisaged time limits for erasure of data and a description of the technical and organisational measures implemented to ensure a certain level of data security based on the risk.

The delegation found that the processing of prospects' and customers' data is part of the company's usual activity, which requires that it hold a record of processing activities in compliance with the provisions of Article 30 of the Regulation.

While the delegation found that the company does keep a record of processing activities, said record does not contain all the information required by Article 30 of the Regulation. In particular, the record does not contain information on:

- the categories of personal data processed;
- the envisaged time limits for the erasure of the different categories of data;
- the categories of data subjects concerned by the processing.

Thus, these actions are in breach of the requirements set out by Article 30 of the Regulation.

In light of the above, the company [redacted], located [redacted], is hereby given formal notice, <u>within three (3) months from the notification of this decision</u> and subject to measures it may already have adopted, to:

- **stop conducting marketing operations targeting individuals whose consent has not been validly collected**, particularly by its partners [redacted], [redacted], [redacted] and [redacted],

- **be able to demonstrate, for each data subject, that their consent to the processing of their personal data by the company for marketing purposes has indeed been collected in advance by its partners**, for example by systematically requiring that partners provide full information on the means and conditions under which consent is collected, in particular the date on which consent is collected, on the physical point of sale or the website on which consent was given and on the product or competition concerned,

- **inform data subjects** in accordance with the provisions of Article 13 of Regulation (EU) by completing the information provided to prospects by telephone, notably on their right to object to the recording of their conversation,

- **hold a record of processing activities containing all required indications,** including the categories of data subjects and the personal data processed as well as the period of storage of such data.

- **justify, to the CNIL, compliance with all of the above requests within the time-limit set.**

After this time-limit, if the company [redacted] has complied with this formal notice, this procedure shall be considered closed and a letter shall be sent to it to this end.

However, if the company [redacted] has not complied with this formal notice, a rapporteur shall be appointed and may request that the restricted committee issue one of the penalties set out under Article 20 of the Act of 6 January 1978, amended.

The Chair

Marie-Laure Denis