Decision no. MED 2019-xx of xxxx issuing formal notice to the company [redacted]

(No. MDM191003)

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 on the free movement of such data;

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to the French Criminal Code;

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 civil liberties, particularly Article 45;

Having regard to Decree no. 2005-1309 of 20 October 2005, amended, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to deliberation n°. 2013-175 of 4 July 2013 adopting the internal regulations of the Commission Nationale de l'Informatique et des Libertés;

Having regard to decision n°. 2018-161C of 26 June 2018 of the Chair of the Commission Nationale de l'Informatique et des Libertés to entrust the Secretary General with carrying out an investigation on the company [redacted] or having such verification mission carried out;

Having regard to records of investigation n°s. 2018-161/1 of 31 July 2018 and 2018-161/2 of 25 October 2018;

Having regard to the other items in the case file;

I. Findings

The company [redacted] (hereinafter "the company"), located [redacted] is a [redacted].It employs [redacted] employees and, in 2017, generated revenues of around [redacted] for a net loss of around [redacted].

The company [redacted] markets [redacted]. Subscribers receive a [redacted] and [redacted] as well as digital access which enriches the magazine with a mobile app.

The company's products target a French customer base but are delivered to several countries, and particularly European countries.For the purposes of its activity, the company runs the [redacted] website (hereinafter "the Website"), through which customers can access their account and subscribe to the company's service.It also runs other versions of the website under national domain extensions (.ch, .co.uk, .be).

On 25 October 2018, the company appointed [redacted] as Data Protection Officer and notified the Commission Nationale de l'Informatique et des Libertés (hereinafter "CNIL" or "the Commission") (declaration n°. DPO-[redacted]).

In accordance with the decision of the Chair of the Commission no. 2018-161C of 26 June 2018, a CNIL delegation carried out on-site investigations on the company [redacted] on 31 July and 25 October 2018.Said investigations were aimed at confirming the compliance with Act n°. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties (hereinafter the "Data Protection Act" or "Act of 6 January 1978, amended") and with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "GDPR") of all of the personal data processing operations pertaining to the marketing and the use of products and services associated with the "[redacted] brand.

By reproducing the account creation process on the company's Website, the investigation delegation found that when the user is asked to provide his/her name and surname, no information on the protection of his/her data is provided, and no link directs the user to the general terms and conditions of sale (hereinafter "the TCs").

On reading these TCs, the delegation found that these do not make any reference to the legal grounds for processing, the right to restriction of processing, to data portability or to the right to submit a claim to a supervisory authority.

On continuing the registration process, the delegation found that passwords are sent to customers in clear text via email. This email contains a link which redirects the user to the company's Website, and allows the user to customise their password. The delegation found that on this occasion a six-figure password such as "123456" was accepted.

After completing the registration process on the company's Website, the delegation found that, in the user account management window, the box corresponding to the option to receive newsletters and marketing emails was ticked by default.

At the bottom of this e-mail is a link to unsubscribe. A click on the link to unsubscribe redirects the user towards a webpage in English, with the title "*Unsubscribe From Messages From* [redacted] and the following text: "*If you no longer wish for XXX to receive any email marketing message from* [redacted] *click Unsubscribe.*, in which XXX is the email address having received the marketing email.

By clicking on the button "*Unsubscribe*" below the text, the user is redirected to a second page, also written in English, containing the following text: "*The email address XXX has been unsubscribed from any future email marketing messages from* [redacted] *If you unsubscribed by mistake, you can re-subscribe by clicking here.*"

The delegation found that after creating an account on the company's Website, users could subscribe to the services offered by [redacted] or ask to receive a test kit. In both cases, the user must fill out a form and provide various elements of personal data, particularly data relating to the [redacted] receiving the kit. This form is not accompanied by any information on personal data protection nor by any link through which the user is invited to learn such information.

During the investigation, the delegation found that the erasure of data on an account can be requested by the customer from their account. These requests are processed by customer service using the [redacted] ticketing management software.

The delegation found that eighteen requests to delete accounts were listed in [redacted]. For at least one of these requests, customer service had answered the requesting individual that "*[their] personal data [had] been erased*" from the company's databases. Yet, the delegation found that this statement was not accurate, and that the customer account still contained personal data in administrative tool [redacted] database (containing information relating to the customer and his/her orders) after stating that they had been erased.

During the investigations carried out, the delegation also found that the computer used by one of the database's administrators to connect to the management tool was configured to never go into "sleep" mode. It also found that one of the company's engineers connects to his Windows session using a six-character password. Lastly, it found that the company's technical manager is able to log in to the ticketing management software by using the customer service manager's account.

Finally, an analysis of the items communicated by the company following the investigation led the delegation to find that passwords were kept after being run through the [redacted] algorithm.

II. Breaches to the provisions of the General Data Protection Regulation

A breach of the obligation to inform data subjects

Firstly, the delegation found that no information relating to personal data protection is communicated in a direct manner upon registering on the company's website or when placing an order. Furthermore, no link is provided to redirect the user to the company's general terms and conditions of sale (hereinafter "the TCs") or privacy policy.

Moreover, said privacy policy is only accessible indirectly, as no link on the website refers the user directly to said policy. To find it, the user must read the TCs. This latter document, as recorded on the day of the investigation, contains an Article 22 on personal data as well as an Article 27.4 which includes a link to the privacy policy.

As regards the obligation of accessibility of information set out in Article 12 of the GDPR, the Article 29 Working Party guidelines on transparency under regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, specify that "*the criteria "easily-accessible" means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it*".

Thus, "*every organisation that maintains a website should publish a privacy statement/notice on the website. A direct link to this privacy statement/notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy policy" or "Data Protection Notice").Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible*".

The data controller must above all take concrete measures to ensure that information is directly provided to the data subject or "*to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.).The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app*".

Secondly, regarding both the TCs and the privacy policy, the user of the company's website is not informed of the legal grounds for processing, nor of his/her right to the restriction of processing and to data portability, or even or his/her right to submit a claim to a supervisory authority.

Nor is the user informed of the data retention period. The company's privacy policy does indeed contain an indication stating that "*data will be kept for the period necessary to provide the service requested by the user, or as set out in the objectives stated in this document*."

In this respect, the guidelines on transparency under Regulation (EU) 2016/679 (WP260 rev.01) adopted on 29 November 2017 and revised on 11 April 2018 explicitly provide in their Annex 1 that: "*the storage period [...] should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/purposes .It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.*"

This constitutes a breach of Article 13 of the GDPR, which requires that the data subject be provided with a certain amount of information relating to the data processing carried out.

This is also a breach of Article 12 of the GDPR, which requires that the data controller "*take appropriate measures to provide any information referred to in Articles 13 and 14 [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]*".

Thirdly, the delegation also found that the newsletter and marketing email sent by the company to its customers or users contains a link enabling them to unsubscribe from this mailing list.

A click on this link redirects users to a page containing text in English, with a button which must be clicked to confirm their unsubscription, also written in English. Furthermore, the page finalising the process to unsubscribe contains a hypertext link titled "*clicking here*" which results in a new subscription to newsletters and marketing emails. The presence of this hypertext link, in English, is of a nature to mislead the user and to make him/her believe that he/she must click to unsubscribe, leading to his/her subscription once more without him/her necessarily being aware.

Yet, the website is drafted targeting an exclusively French audience and only offers French content, both on its website and in the leaflets that the company distributes. In this respect, the Article 29 Working Party guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, specify that "*the requirement that information is "intelligible" means that it should be understood by an average member of the intended audience*" and that "a translation in one or more other languages should be provided where the controller targets data subjects speaking those languages".

This is a breach of Article 12 of the GDPR, which requires that the data controller "*take appropriate measures to provide any information referred to in Articles 13 and 14 [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]*". This article also provides that "*the data controller shall facilitate the exercise of data subject rights under Articles 15 to 22*".

A breach of the obligation to comply with the request to erase data

The delegation found that on the date of the investigation, requests to erase data were not systematically followed by the effective erasure of concerned customer or users' personal data, for requests going back at least five months. It was also found that the company's customer service had informed users that their personal data had been erased despite the erroneous nature of this statement.

Although certain data can be kept under legal requirements or for purposes of proof following a request for erasure, the keeping of unnecessary data despite a data subject exercising his/her rights is a breach of the provisions of Article 17 of the GDPR, which provides that "*the data subject shall have the right to obtain from the data controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay*".

A breach of the obligation to ensure the security of data

Firstly, as regards passwords, the delegation found that upon creating an account on the company's Website, a seven-character password containing only lowercase and uppercase letters is sent to the user by email, in clear text. When changing the password received, a six-character password is accepted.

It appears from these elements that the security measures in place are not enough to ensure a sufficient level of security and confidentiality given that the passwords used to create a customer account are comprised of only two types of characters (digits and letters), and can be only six characters long.

In fact, authentication based on the use of an insufficiently complex password can lead to the associated accounts being compromised and attacked by non-authorised third parties. Yet, these accounts contain personal data.

Secondly, the delegation was informed that passwords are kept after being run through the [redacted] algorithm, which is now considered [redacted]

It arises from these elements that the company's password management policy does not include sufficient and stringent measures to ensure the security and confidentiality of the data to which they allow access.

As regards the locking of workstations, the delegation found that the computer used by one of the database's administrators to connect to the management tool was configured to never go into "sleep" mode. This configuration means that the user's session is never automatically locked after a prolonged period of no use, e.g. after the employee leaves his workstation, and that third parties can access the data processed on said computer.

As regards access to data, the delegation found that the company's technical manager is able to log in to the ticketing management software by using the customer service manager's account. The absence of specific identification does not make it possible to ensure access traceability or that data are accessed only by those persons responsible for processing said data as part of their job.

This constitutes a breach of Article 32 of the GDPR which provides that "*the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

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

The delegation found that, upon registering on the company's Website, the user is automatically subscribed to newsletters and marketing emails, even in the case in which he/she has not taken out any subscriptions and is therefore not one of the company's customers.

This constitutes a breach of the provisions of Article 13 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector- which provides that "*the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent*" - and of the provisions of Article L.34-5 of the French Postal and Electronic Communications Code- which *provides that "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*".

In the absence of an order placed by the data subject, the company cannot validly invoke the benefit of the exception created by these texts which allows for marketing without prior consent when the recipient's contact details have been collected from said recipient for a sale or the provision of a service when such direct marketing concerns similar products or services provided by the same natural or legal person.

Thus, the company must collect the specific consent of users prior to any electronic marketing operations.

In light of the above, the company [redacted] located [redacted] in [redacted] ([redacted]), <u>is hereby given formal notice</u>, within two (2) months from the notification of this decision and subject to measures it may already have adopted to:

- **inform data subjects, pursuant to the provisions of Articles 12 & 13 of the GDPR, about personal data processing activities set up, and in particular:**
  - **provide users with this information in an easily accessible manner on the forms used to collect personal data**, e.g. by providing at the bottom of these forms information on the data controller's identity, on the purposes of the processing and on the rights of data subjects, and by inviting users to view full and detailed information through a clickable link;
  - **provide full information,** for example in the Website's privacy policy accessible on the [redacted] website, mentioning all of the required information set out in Article 13 of the GDPR;
  - **set up a procedure for unsubscribing from the newsletter and marketing email that is compliant** with the provisions of Articles 12 and 21 of the RGPD, which can be understood by the users in question, written in the relevant language (in French for users of the website located in France) to ensure its effectiveness;
- **ensure, under the conditions set out in Article 17 of the GDPR, the effectiveness of all requests to exercise the right of erasure** made by data subjects whose data are processed by the company, and in particular, for older company customers, the erasure of their data, subject to those that must be temporarily archived under legal and litigious obligations;
- **take any security measure, for all types of processing of personal data carried out, for protecting the security of said data and preventing access thereto by unauthorised third parties,** in accordance with the provisions of Article 32 of the GDPR, not least by:
  - setting up a restrictive policy as regards the passwords used by the website users, particularly in terms of complexity (minimum of 12 characters including at least one lowercase, one uppercase, one digit and one special character, if there are no additional measures) and storage by using a robust hashing algorithm);
  - no longer sending passwords in clear text by email, especially during creation of a user account;
  - ensuring that the company's workstations go to sleep without fail, requiring a password to be entered to log in to the session again;
  - setting up individual accounts specific to each person with access to the company's tools, not least the ticketing management software;
- **do not process data for direct electronic marketing purposes without first having obtained the freely** given, specific and informed consent of data subjects who are not customers of the company, pursuant to the provisions of Article L34-5 of the French Postal and Electronic Communications Code, not least by ensuring that prior consent is obtained (e.g.: box to tick) and by no longer targeting data subjects who have not given their consent;

- **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 measures set out under Article 45 of the Act of 6 January 1978, amended.

The Chair

[redacted]