Decision No. MED 2021-089 of 16 September 2021 issuing an order to the company [redacted]

(MDM No. 211104)

The Vice Chairman of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, in particular Articles 56 and 60;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Decision No. 2013-175 of 4 July 2013 adopting the rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2018-202C of 28 September 2018 of CNIL's Chair to instruct the secretary general to carry out or have a third party carry out an assignment to verify the processing implemented via the [redacted] domain or related to personal data collected by it, through any organisation that may be concerned by the use of such data;

Having regard to the online findings report No. 2018-202/1 of 1 October 2018 and No. 2018-202/2 of 11 February 2020;

Having regard to the hearing report No. 2018-202/3 of 3 March 2020;

Having regard to the other documents in the file;

I. <u>Background and procedure</u>

Created in 2009, the company [redacted] located at [redacted], is a limited liability company specialising in the rental of holiday homes and apartments abroad, mainly in Spain. It recently developed its activities in France, Italy and Portugal. The company has [redacted] employees and generated turnover of [redacted].

The company publishes the website [redacted] and connects rental agencies with individuals. Those agencies pay the company a commission for reservations made using the [redacted] website. In 2018, 1275 reservations were made.

The [redacted] domain is divided into several subdomains, the versions of which are identical:

- [redacted] is the French version of the website;
- [redacted] is the Spanish version;
- [redacted] is the English version of the site.

In 2018, CNIL received an internal report, informing it that files containing personal data and unencrypted passwords are allegedly freely accessible and downloadable without prior authentication on the website, [redacted]

Pursuant to the Decision No. 2018-202C of 28 September 2018 of the CNIL Chair, a delegation carried out two online verification missions on 1 October 2018 and 11 February 2020, in order to verify the compliance of any processing accessible from the domain [redacted] or concerning personal data collected from it from any organisation concerned by their implementation under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the Regulation or the GDPR) and the amended Act of 6 January 1978 (French Data Protection Act). These two verification missions were followed by a hearing on 3 March 2020, followed by a questionnaire sent to the company on 27 May 2020.

In the context of on-line verifications, this included checking the information procedures for provision of information to individuals and data security. The hearing and questionnaire made it possible to clarify the findings made during the inspections. Additional information was provided by the company on 3 and 18 October 2018, as well as on 10 March and 18 June 2020.

On 6 July 2021, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

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

II. Breaches with regard to the provisions of the GDPR

A breach of the obligation to collect data for specified, explicit and legitimate purposes

Article 5(1)(b) of the GDPR provides that personal data must be collected "*for specified, explicit and legitimate purposes*".

The delegation was informed by the company that it collects email addresses via a "newsletter" field on the home page of the [redacted] website. The delegation noted that 263 email addresses collected from the "newsletter" fieldare present in the database.

However, the company stated that it no longer used that data, insofar as it does not send any newsletter or advertising to prospects.

By collecting personal data that it does not use, the company collects data for no purpose, in breach of Article 5(1)(b) of the Regulation. It is therefore up to the company to stop the collection of email addresses via the "newsletter" field and delete the email addresses previously collected via that field.

Breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing

Article 5(1)(e) of the GDPR provides that personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*".

The CNIL recalls that the retention period of personal data must be determined according to the purpose pursued by the processing. Where the data is no longer necessary for the purpose for which it was collected, the data must either be deleted, or be subject to intermediate archiving when the data is necessary for compliance with legal obligations or for pre-litigation or litigation purposes. The data thus placed in intermediate archiving are then archived for a period not exceeding that necessary for the purposes for which they are stored, in accordance with the provisions in force. Thus, after having carried out a sorting of relevant data to be stored, the data controller must provide for this purpose a dedicated archive database or logical separation in the active database. This logical separation is ensured by the implementation of technical and organisational measures ensuring that only persons with an interest in processing the data due to their duties can access them. Beyond such data retention periods in intermediate archive, personal data must, unless otherwise provided, be deleted or anonymised.

Thus, in the context of commercial activities, customer and prospective data may be reasonably retained for a period of three years from the end of the business relationship, considered as the last purchase or contact from the user. At the end of this period, the CNIL recommends that such data be deleted.

First, the delegation was informed that the client data was kept for ten years because they are linked to reservation contracts to be retained for such a period for tax and accounting purposes. At the end of that period, the company carries out a “cleaning” of the data in order to keep only the name of the users. The company informed the delegation that it retains the names of users indefinitely in order to have a means of searching in its database in case of administrative or commercial need.

In this respect, the delegation noted that the names of 10,730 customers whose last reservation was over ten years ago were retained without a time limit.

However, the CNIL recalls that a retention period must be set according to each purpose and that under no circumstances must personal data be kept for an indefinite period.

Thus, the retention of the names of the company's customers beyond ten years and for an indefinite period is excessive with regard to the purposes related to administrative or commercial needs.

Secondly, the delegation was informed that the company retains the data of prospects for a period of five years, “*fixed arbitrarily*”. In this context, prospects are those who have started a reservation process without finalising it or having issued an accommodation selection request. The company has specified that this retention was for the purpose *“of internal commercial use, in order to better target our responses to new selection requests from customers*”.

However, the fixed retention period must be necessary with regard to the purposes for which the personal data are processed. The retention of such individuals’ data for five years for “*internal commercial use*” appears to be excessive, since the company can improve its offers by studying unfinished and anonymous requests.

Thirdly, the delegation was also informed that no procedure for the intermediate archiving of customer data or access restriction was implemented within the company.

All of these facts constitute a breach of Article 5(1)(e) of the GDPR. It is therefore up to the company to set data retention periods for its customers and prospects that are proportionate to the purposes for which such data was collected. It is also up to it to implement an intermediate archiving procedure for its customers' data, with restricted access.

A breach of the obligation to inform persons

Firstly, Article 12 of the GDPR provides that "*The controller shall 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*".

With regard to the transparency of information, the guidelines of the "Article 29" Working Party (now the European Data Protection Board) on transparency within the meaning of Regulation (EU) 2016/679, adopted on 29 November 2017, specify, concerning information, that the information "*This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues (...)*'. The Guidelines add that "*The data subject must not have to actively search for information covered by [Articles 13 and 14] amongst other information, such as terms and conditions of use of a website [...]*".

However, the delegation found that the information of individuals relating to the processing of their personal data is contained in the "Terms of Service" ("TOS") of the [redacted] website, among other information not related to personal data protection.

Therefore, the procedures for providing information on personal data protection do not meet the transparency requirements laid down in the Regulation.

Concerning the accessible nature of the information, the aforementioned guidelines also state that "*The 'easily accessible' element 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, [or] by linking them to it*".

These guidelines illustrate the need for the data controller to take concrete measures to ensure that the information is provided directly to the data subject or to actively direct that person to the location of such information.

However, the delegation found that the information relating to personal data collected during the creation of a user account was not easily accessible. Indeed, although as part of the Terms of Service located at the bottom of the [redacted] website, this information is not directly brought to the attention of the data subjects, whether on the website's collection pages or via a clickable link inserted on the collection page referring to a document containing that information.

It follows from the above that both transparency and accessibility of the information provided to the data subjects are lacking in the present case.

Secondly, Article 13 of the GDPR provides that different information is provided to the data subject at the time of the collection of personal data concerning them.

However, the delegation found that the following mandatory information was absent from the Terms of Service of the [redacted] website:

- The existence of the right to ask the data controller to limit data processing associated with a data subject, the right to object to processing, and the right to data portability;
- Data retention periods;
- The right to lodge a complaint with a supervisory authority;
- The legal basis for processing.

All of these facts constitute a breach of Articles 12 and 13 of the Regulation. It is therefore up to the company to include the information required by Article 13 of the Regulation in a dedicated medium, such as a privacy policy, and to bring such information to the attention of the users of its website, either directly on the personal data collection pages or by means of a clickable link to the privacy policy. The latter must also be supplemented in order to contain all the information required by Article 13 of the Regulation.

A breach of processing obligations

Article 28 of the Regulation provides that the processing carried out by a processor for a data controller is governed by a contract which determines the conditions under which the processor undertakes to carry out the processing operations on behalf of the data controller.

In accordance with Article 28 of the Regulation, that contract specifies the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, and the categories of data subjects, and the data controller's rights and obligations. That contract must in particular provide that the processor only processes personal data on documented instructions from the data controller.

In this case, [redacted]is responsible for hosting the [redacted] website and for server management, while [redacted] is the [redacted]'s payment provider. In this context, they process personal data on behalf of [redacted]. As such, these two companies are processors of [redacted] within the meaning of Article 4 of the GDPR.

However, the delegation found that the service contracts binding these two service providers to [redacted] did not contain any of the provisions required by Article 28 of the GDPR.

These elements combined constitute a breach of Article 28 of the GDPR. It is therefore up to the company to supplement the contracts concluded with its processors in order to include all the information required by this article, which specifies the obligations incumbent upon them in terms of the protecting the security and confidentiality of your customers' data.

A breach of the obligation to ensure the security and confidentiality of personal data

Article 32 of the Regulation provides in particular that "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

Firstly, the delegation was informed that the production data, which correspond to actual data, were imported three to four times a year into the database for testing.

However, the CNIL considers that the use of fictitious or anonymised data in the context of IT testing constitutes an essential security precaution to be adopted in terms of IT developments.

Secondly, the company has set up a password hash for the user accounts of the [redacted] website using the MD5 + salt algorithm.

However, the CNIL recommends using hashing algorithms deemed strong for the storage of passwords, with the MD5 + salt function being deemed obsolete (Decision No. 2017-012 of 19 January 2017 adopting a recommendation on passwords).

Thirdly, the delegation found that a user account could be created on the [redacted] website using a password consisting of a single character. No complex password rules or additional measures have been put in place.

Similarly, in the context of the hearing of 3 March 2020, the company stated that access to the new development server [redacted] was obtained by means of a password consisting of 8 characters, including 2 different types of characters (lower case and number) and that no additional measures were put in place.

However, the password characteristics defined by the company do not ensure a sufficient level of personal data security. Indeed, authentication based on the use of an insufficiently complex password can lead to the compromising of the associated accounts and attacks by unauthorised third parties, for example “brute force” attacks which consist of systematically testing many passwords successively.

In this respect, the CNIL's decision on passwords recommends that passwords consisting of 8 characters contain 3 of the 4 character types (upper case letters, lower case letters, numbers, and special characters) and be accompanied by an additional measure such as the timing out access to the account after several failures or an account locking measure after a maximum of ten unsuccessful login attempts.

Fourthly, the delegation found that the current production database is based on an obsolete version (mySql, October 2010), which is no longer subject to security updates in case of vulnerability.

However, the CNIL recommends that regular monitoring and updating of the technical and application components be carried out, particularly on websites, servers, databases, and workstations.

All of these facts constitute a breach of Article 32 of the GDPR. It is therefore up to the company to stop using actual data in the context of IT testing, to use a hashing algorithm deemed strong for the storage of passwords, to define password complexity rules for users of its site to ensure a sufficient level of security of their personal data and to regularly update the database of technical and application components.

Consequently, [redacted], located at [redacted] is hereby ordered, <u>within 3 months of notification of this Decision</u>, and subject to any measures it may have already adopted, to:

- **only process personal data for specific, explicit and legitimate purposes,** particularly by ceasing to collect email addresses via the "newsletter" field on the homepage of the [redacted]_website, and by deleting the email addresses previously collected;

- **define and implement a data retention period policy relating to the company's customers and prospects which does not exceed the duration necessary for the purposes for which they are collected,** and implement an effective procedure for archiving the processed data with restricted access;

- **inform the data subjects,** in accordance with the provisions of Articles 12 and 13 of the Regulation, about the personal data processing put in place, particularly by providing users:

  - complete information, in a dedicated document, on the personal data processing implemented;
  - transparent and directly accessible information on the forms from which personal data are collected;

- **provide in all contracts between the company and its service providers,** in particular [redacted] and [redacted], clauses specifying the obligations incumbent on the service providers with regard to protecting the security and confidentiality of the company's customers' data, and specifying in particular that service providers may act only on instructions from the controller, in accordance with Article 28 of the Regulation;

- **to take all security measures, for all personal data processing operations, to protect the security of such data and prevent unauthorised third parties from accessing it pursuant to Article 32 of the GDPR, and** in particular:
  - **with regard to the production data imported into the development database in order to conduct testing:**
    - cease using actual personal data for the development and testing phases;

  - **with regard to passwords:**
    - for instance, passwords consist of a minimum of 12 characters, containing at least one upper case letter, one lower case letter, one number, and one special character; **<u>or</u>**
    - passwords are composed of at least 8 characters, containing 3 of the 4 character types (upper case letters, lower case letters, numbers, and special characters) **<u>and</u>** are accompanied by a supplemental measure such as timing out access to the account after several failures (temporary access suspension whose duration increases as attempts are made), the establishment of a mechanism to guard against automated and intensive submission of attempts (for example: "captcha") and/or the locking the account after several unsuccessful authentication attempts (maximum 10);

    - use a recognized and secure algorithm, such as for example bcrypt, scrypt or PBKDF2, and, where applicable, the use of a salt, for the storage of passwords in the database;

  - **regularly monitor and update** the technical and application components on websites, servers, database, workstations, etc.;

- **Provide supporting documentation to the CNIL that all of the aforementioned claims have been complied with within the time limit set.**

At the end of that period, if [redacted] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

Conversely, if [redacted] has not complied with this order by the end of that period, a rapporteur will be appointed who may request the restricted committee to issue one of the sanctions provided for by Article 20 of the amended Act of 6 January 1978.

The Vice-President

[redacted]