CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The President

[redacted]

Paris, on 5 décembre 2024

Our ref.: [redacted]
To be stated in all correspondence

Registered letter with acknowledgement of receipt no. [redacted]

Dear Sir,

[redacted]'s main activity is the marketing of travel services (flights, hotels, holidays, cruises, etc.) via its website "[redacted]" and its mobile application "[redacted]". It offers its services in several European Union countries.

In accordance with my **decision no. 2024-026C of 27 December 2023**, on 29 February 2024 the Commission nationale de l'informatique et des libertés (CNIL) carried out an online inspection of the website accessible from the URL "[redacted]" published by [redacted]. This inspection continued with an online inspection on 6 and 11 March 2024 and a hearing at the CNIL's offices on 21 March 2024.

The purpose of this inspection was to verify the compliance of the processing operations carried out by [redacted] with the provisions of Regulation (EU) 2016/679 on data protection (GDPR) and Law No 78-17 of 6 January 1978 ("Data Protection Act") as amended. In particular, we checked the procedures for unsubscribing from the [redacted] newsletter and the data retention periods.

The findings of these inspections, together with the additional information provided on 3 March, 12 April, 5 June and 4 July 2024, lead me to make the following observations.

Firstly, on the corrective actions implemented

In a letter dated 19 March 2024, [redacted] informed the CNIL delegation that, prior to the online inspection, it had "*initiated a compliance initiative for the processing of personal data*" and that it had implemented corrective measures on the basis of the online findings made by the CNIL delegation.

I have therefore taken note of the fact that the cookies banner displayed on the "[redacted]" website has been made compliant during the course of the procedure, to enable users to refuse the placement of cookies easily and with a single click, and also to modify the settings for advertising cookies, which are no longer activated by default following the inspection procedure. As a result, I note that no cookies subject to prior consent are deposited on the user's terminal as soon as they arrive on the "[redacted]" website and before any action is taken on their part.

I also note that the technical malfunction of the unsubscribe link inserted in [redacted] newsletters, which affected 2.2% of your marketing campaigns, was corrected on 15 March 2024.

The delegation also noted, at the hearing on 21 March 2024, that the prior consent of individuals to receive [redacted] newsletters is now specifically sought on the form used to create a member account.

In addition, in support of the corrective measures announced by your company, on 12 April 2024 you sent the CNIL delegation an action plan with an implementation schedule. In this respect, I note the deployment in June 2024 of action no. 13, the purpose of which is to fulfil your security obligation concerning the methods for automatically connecting members to their account.

Finally, in the supplementary information provided on 4 July and 2 August 2024, the delegation noted that [redacted] had updated its password policy, which now has to be at least 8 characters long with at least one special character, one upper case letter, one lower case letter and one number, with authentication subject to an additional measure.

I. Analysis of the facts in question

1. On the failure to comply with the obligation to define and comply to a retention period proportionate to the purpose of the processing operation

Article 5(1)(e) GDPR states 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* [...]".

Article 5(2) of the GDPR states that the "*controller shall be responsible for, and be able to demonstrate compliance with [of Article 5 of the GDPR]*".

In the specific case of the retention of data linked to a user account created on a website, this can in principle be retained until the account is deleted.

However, users often stop using these accounts without deleting them, which means that they continue to exist indefinitely. In this case, the principle of limited retention of personal data requires the controller to determine a reasonable period of time after which, if there has been no activity on the part of the user, the account must be considered as inactive and must be deleted, along with the personal data linked to it.

In this respect, the CNIL considers, in its reference framework relating to personal data implemented for the purposes of managing commercial activities[1], that a period of two years is proportionate. It is advisable to warn the users concerned before deleting the accounts of those who have not reacted within the time limit set by the organisation.

In this case, the inspection delegation was informed that data from member accounts (customers and non-customers) on the '[redacted] platform" was being kept for an unlimited period.

[1] https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_traitements-donnees-caractere-personnel_gestion-activites-commerciales.pdf

Therefore, the delegation noted in the [redacted] customer data management tool the presence of 6,473,236 member accounts that had not interacted (connected to the account or clicked on a link in the newsletter) with [redacted] for more than five years.

In addition, [redacted] informed the delegation that a technical incident at the end of May 2021 on the database of users of the "[redacted]" platform resulted in the date of their last connection being reset to the end of May 2021. Therefore, 6,855,108 member accounts were affected by the incident. In its response of 5 June 2024, [redacted] stated that since this incident, the last connection date is correctly updated with the new date in the database provided that the user connects (or attempts to connect) to their account again.

Consequently, this data alteration does not allow [redacted] to check, for the affected accounts, the actual date of last activity (last connection to the account) in order to implement a retention period policy in the database, except if the user connects to their account again.

I therefore consider that [redacted] has failed to comply with the provisions of Article 5(1)(e) of the GDPR by keeping member account data for an unlimited period, and with Article 5(2) of the GDPR since, given the current configuration of the database, even if [redacted] wished to comply with the defined retention period, it would not be able to demonstrate this.

However, I note that corrective actions are underway to formalise a retention period policy and implement it.

Nevertheless, the measures announced call for the following observations. A retention period of five years from the date their account was created for data on member accounts that have never ordered on the "[redacted]" platform seems excessive given that the only justification put forward is to enable your company to retain the member account interface in the event of the account being reused. A shorter retention period should be set, in order to better guarantee compliance with the principle of limiting retention periods set out in Article 5 of the GDPR.

In addition, I would remind you that the retention of customer member data in intermediate storage should only concern billing data and only if your company is legally obliged to do so (for example, to meet accounting or tax obligations) or if it wishes to build up evidence in the event of a dispute, and within the limit of the applicable limitation period.

2. <u>On the breach of the obligation to ensure data security and confidentiality</u>

In law, Article 32(1) of the GDPR states: "*Having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons, the controller and the processor will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [....].*"

In this regard, the CNIL recalled that the implementation of a robust authentication policy constituted an elementary security measure that generally contributed to compliance with the obligations of Article 32 GDPR (CNIL, FR, 24 November 2022, Sanction, No SAN-2022-021, published). Thus it was necessary to ensure that a password that could be authenticated on a system could not be disclosed.

In its Deliberation No 2022-100 of 21 July 2022 adopting a recommendation on passwords and other shared secrets, which is not mandatory but which provides relevant information on the security measures that should be taken, the CNIL recommends that, to ensure a sufficient level of security and confidentiality, if authentication is based solely on an identifier and a password, the password be composed of at least 12 characters including upper case, lower case, numbers and special characters to be chosen from a list of at least 37 possible special characters, or be composed of at least 14 characters including upper case, lower case and numbers, without any mandatory special character, or, when it corresponds to a sentence comprising words in the French language, be composed of at least seven words.

Failing this, the CNIL considers that a sufficient level of security and confidentiality can also be ensured by authentication based on a password at least eight characters long, made up of three different categories of characters but accompanied by an additional measure such as, for example, a temporary ban on access to the account after several unsuccessful attempts, the duration of which increases with each attempt, the implementation of a mechanism to protect against automated and intensive submissions of attempts (e.g. "captcha") or the blocking of the account after several unsuccessful authentication attempts (maximum 10).

In this case, the delegation noted during the online inspection of the "[redacted] website that the password policy did not impose a certain level of complexity when creating a user account. The delegation was therefore able to define a password such as "123456".

I therefore consider that [redacted] breached the provisions of Article 32 because the passwords used for existing member accounts to access the [redacted] platform were not sufficiently complex.

However, I note that remedial actions are underway to update the level of password complexity for member accounts registered before the start of the phased inspection process from June 2024.

II. Corrective measures ordered by the CNIL (Article 20 of the Act of 6 January 1978)

Due to all these elements and, in agreement with the other data protection authorities concerned by this processing, it is therefore necessary to order the following corrective measures against [redacted]

- **A REMINDER OF LEGAL OBLIGATIONS**, in accordance with the provisions of Article 20 of the Law of 6 January 1978, concerning the obligation to demonstrate compliance with retention periods, given the alteration in the database of the field relating to the date of last activity of member accounts, in accordance with Article 5(2) of the GDPR.

- **FORMAL NOTICE** in accordance with the provisions of Article 20 of the Law of 6 January 1978, within **three (3) months of notification of this decision and subject to any measures it may have already adopted, to:**

  - **define and implement a retention period policy for data relating to your company's members** that does not exceed the period necessary for the purposes for which it is collected, in particular for data relating to inactive members' accounts, in accordance with Article 5(1)(e) of the GDPR;

- **take all security measures**, for all processing of personal data that it implements, to safeguard the security of such data and prevent unauthorised third parties from gaining access to it, in accordance with the provisions of Article 32 of the GDPR, in particular by imposing sufficient complexity on passwords for existing member accounts as recommended by the CNIL.

This formal notice, which does not require a response from you, entails the closure of procedure No 2024-026C. However, this closure is without prejudice to the right reserved by the CNIL to carry out a new verification mission, in order to check that your company has complied with this formal notice on expiry of the time limit.

In the event of a new verification procedure, if your company has not complied with this formal notice, a Rapporteur will be appointed who may ask the Restricted Committee to impose one of the penalties set forth in Article 20 of the French Data Protection Act.

This decision may be appealed before the Conseil d'État within two months of its notification.

For more information on the formal notice procedure, you can consult the CNIL website at: https://www.cnil.fr/fr/la-procedure-de-mise-en-demeure-0.

The CNIL's departments, [redacted] the Inspections Department [redacted] in the Inspections Department [redacted] are at your disposal for any further information you may require.

Sincerely,

[redacted]

Marie-Laure Denis