CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The Chair

Registered letter with acknowledgement of receipt
AR ref. no: 2C 137 386 12G 8

[redacted]

Paris, 28 NOV. 2022

Investigation of the case:
[redacted]
Ref. No.: [redacted]
Referral [redacted]
(to be quoted in all correspondence)

Dear Madam,

I am following up on the exchanges between CNIL and your data protection officers (DPO) as part of the investigation of [redacted]'s complaint, which was forwarded to us by the Italian data protection authority pursuant to Article 56.1 of the General Data Protection Regulation (GDPR).

This complaint concerns illegitimate access to the complainant's personal data made available on her customer area accessible from the website [redacted] It also concerns the exercise of the right of access vis-à-vis [redacted] and the lack of response.

The processing of the personal data in question is cross-border within the meaning of Article 4 of the GDPR and therefore falls under the European cooperation mechanism (known as the "one-stop shop") pursuant to the provisions of Article 56 of the Regulation. CNIL acts as the lead authority for this processing carried out by [redacted].

The exchanges with your DPOs have led me to note the following elements.

1. **Security of processing**

Pursuant to the GDPR, personal data must be used in such a way as to ensure its security, including protection against processing that would be unauthorised or unlawful, including appropriate technical or organisational measures (Article 5.1 f) GDPR). The data controller must thus guarantee a level of security appropriate to the risk, in order to guarantee the confidentiality, integrity, availability and constant resilience of the processing systems and services (Article 32 GDPR).

In the event of a personal data breach, the data controller must notify the competent supervisory authority (Article 33 GDPR) and inform the data subjects when it is likely to result in a high risk to their rights and freedoms (Article 34 GDPR).

In this case, I note first of all that [redacted] notified CNIL of the data breach on 3 February 2020 ([redacted] supplemented on 19 March 2021 by a subsequent additional notification (no. FR2103191400001). In addition, all data subjects were informed by email on 17 February 2020.

Secondly, it was indicated to CNIL that this incident, identified on 31 January 2020, originated from "*an update of* [redacted] *websites, particularly the web cache system, aimed in particular at speeding up the display of information pages on reservations on 28/01/2020*". Indeed, it was stated that "*the technical*

optimisation proved to be defective", which enabled customers clicking on "*a link contained in the email messages received from* [redacted] *prior to their trips*" to "*see, in some specific cases, the content of bookings from other passengers*".

I also note that investigations were carried out by you which revealed that 147 reservation files, known as "PNR", were affected by the incident, corresponding to 174 passengers with an [redacted] ticket. The data concerned relate to the identification of passengers, their contact details, their PNR reference number and travel data.

You have specified that three days after the incident was discovered, then on 15 February 2020, technical and organisational measures to correct the defective update were implemented, making it possible to limit the loss of confidentiality induced by the breach and to ensure adequate security of the personal data of the customers concerned for the future.

In this regard, I note the prompt implementation of corrective measures to limit the disclosure of data relating to your customers, which appears to have been a necessary action to respond to this data breach.

However, although "*the risk appeared to be limited*"- according to your company in view of the nature of the data concerned and the short duration of the incident, the fact remains that the elements brought to the attention of the CNIL show that the implementation of such an update, which proved to be defective in this case, was not surrounded by sufficient guarantees to ensure that it was implemented in accordance with the legislation on data protection.

I therefore consider that, despite the implementation of appropriate corrective measures prior to the breach, [redacted] has failed to comply with Article 32 of the GDPR by not taking sufficient measures to guarantee the security and confidentiality of the personal data processed as part of the management of ticket reservations and the sale of ancillary products when updating the [redacted] websites.

We note that, "*as a security measure*", you have allocated "*new booking references for customers who had an upcoming flight*".

The aforementioned facts justify the pronouncement against [redacted] of a reprimand.

2. The complainant's request for access

Pursuant to the GDPR, the data controller is required to respond to a data subject making a request pursuant to articles 15 to 22 of the GDPR, indicating the measures taken as a result of his or her request as soon as possible "*and in any event within one month of receipt of the request.*" (article 12.3 of the GDPR).

Thus,Article 15.1 of the GDPR provides for the right of an individual to obtain confirmation from the data controller as to whether or not personal data relating to him or her are being processed and, where they are, access to the personal data relating to him or her including "*any available information as to their source*" where the data are not obtained from the individual. Paragraph 3 of the same article also provides that "*the data controller shall provide a copy of the personal data undergoing processing*".

In this case, [redacted] exercised her right of access to the data concerning her held by [redacted] on 31 January 2020. [redacted] staff responded to it on 13 July 2021 following an intervention by CNIL to your DPO, more than seventeen months after her request.

I therefore consider that [redacted] has failed to comply with Articles 12 and 15 of the GDPR in that it was unable to provide [redacted] with a response to her request for access within one month.

These facts justify the pronouncement against [redacted] of a reprimand.

3. Corrective action pronounced by CNIL (Art. 58-2 GDPR)

Due to all of these elements, and in agreement with the other data protection authorities affected by this processing operation which have been consulted, the following corrective action must therefore be ordered against [redacted]:

- **A REPRIMAND,** in accordance with the provisions of article 58.2. b) of the General Data Protection Regulation and article 20.II of the law of 6 January 1978 as amended, with regard to the absence of sufficient measures to ensure the security of personal data when updating the company's websites and failure to respond to a request for access within one month.

I would like to point out that this decision, which closes the investigation of [redacted]'s complaint, does not preclude the CNIL from making use, particularly in the event of new complaints, of all the other powers attributed to it by the GPDR and by the amended Act of 6 January 1978.

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

Yours sincerely

[redacted]

Marie-Laure Denis

Copy to:

[redacted], Data Protection Officer