The Chair

THE CHAIRMAN
[redacted]

Paris, 17th June 2025

By recorded delivery letter

References to be stated in all correspondence:
[redacted]

Dear Sir,

I am following up on the exchanges that took place between your company and the French National Commission for Information Technology and Civil Liberties (hereinafter "CNIL") after receiving complaint no. [redacted] forwarded by the German data protection authority of the state of Baden-Württemberg pursuant to Article 56.1 of the General Data Protection Regulation (GDPR).

As a reminder, on 14 August 2023, the German authority in Baden-Württemberg forwarded to the CNIL a complaint from one of its nationals against your campsite [redacted]

This complaint reported the theft of your company's safe containing customer identity documents and the fact that all these customers were sent a copy of the report recording the filing of the complaint (which included the personal data of all the victims).

By email dated 3 April 2024, the CNIL informed you that it had received this complaint, indicated that the transmission of the complaint report containing the identity details of all the individuals affected by the theft constituted a data breach on your part as data controller, and requested your comments within one month.

On 18 April 2024, you confirmed that you had forwarded the complaint report containing their identity details to all data subjects affected by the theft.

Pursuant to Article 60(3) GDPR, the draft decision was forwarded to the European concerned supervisory authority on 7 May 2025.

On 4th June 2025, that draft decision did not give rise to any relevant and reasoned objections from the concerned supervisory authority, so that, pursuant to Article 60(6) of the GDPR, it is deemed to have approved it.

I. The breaches in question

a. Breach of the obligation to process data that is adequate, relevant and necessary with regard to the purposes for which it is processed

In law, Article 5(1)(c) GDPR states that personal data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"*.

The data controller must therefore comply with the principle of data minimisation by refraining from collecting, storing or, more generally, processing data that is not necessary for the purposes pursued.

In this case, your company collected and stored identity documents such as passports, driving licences and identity cards belonging to customers of its campsite in a safe to ensure that they would pay the amounts owed at the end of their stay.

However, collecting customers' identity documents for the entire duration of their stay as a guarantee of payment of camping fees does not appear to be adequate, relevant or necessary in view of the purpose pursued.

Less intrusive means commonly used by tourist establishments, such as taking a deposit, a bank card imprint or a cheque, to be returned at the end of the stay, were available to achieve the purpose pursued, namely, to guarantee payment.

The fact that the prefecture authorised such a practice has no bearing on the inadequacy, irrelevance or necessity of the data collected.

Consequently, I consider that there has been a breach of Article 5(1)(c) of the GDPR.

b. Breach of the obligation to process data in a manner that ensures appropriate security

In law, Article 32 GDPR provides that: *"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."

A breach of this provision includes, in particular, a breach of data confidentiality resulting from the loss or disclosure of data.

In this case, firstly, your company was the victim of a safe theft on 7 August 2023, between 5 a.m. and 7 a.m., containing approximately 363 identity documents belonging to your customers. It appears from your complaint that the door to the reception area where the safe was located was forced open by two men.

It also appears that no special security measures were taken to prevent the theft and that no member of staff intervened to prevent it, even though the safe contained sensitive documents proving the identity of approximately 363 people and creating a high risk of identity theft.

In view of the above, I consider that your company has not implemented appropriate security measures to protect the personal data contained in the safe from theft, despite the sensitivity of the authentic identity documents it contained.

Secondly, it appears from exchanges between the CNIL and your company that the latter sent all its customers affected by the theft a report containing the following personal data: name and place of residence, town, postcode and country of all data subjects affected by the theft.

Each of the customers affected by the theft was thus informed of the names and addresses of all the other customers whose identity documents had been stolen.

I consider that your company did not process this data in such a way as to guarantee its security – in particular its confidentiality – but, on the contrary, participated in its disclosure.

All of these elements indicate that there has been a breach of Article 32.

II. Corrective measure imposed by the CNIL

In view of all these factors, I consider that the following corrective measure should be issued to [redacted]:

- **A REPRIMAND**, in accordance with the provisions of Article 58(2)(b) of the General Data Protection Regulation and Article 20.III of the amended Act of 6 January 1978, concerning the obligations of the data controller to process data that is adequate, relevant and necessary in

light of the purpose of the processing and to process the data in a manner that ensures appropriate security.

I would point out that this decision does not preclude the CNIL from using all the other powers conferred on it by GDPR and the amended Act of 6 January 1978, particularly in the event of complaints.

This decision may be appealed before the Council of State within two months of its notification.

The Commission services (the Registry of the Sanctions and Litigation Department – (01.53.73.22.41/22.53/22.64) are at your disposal for any further information.

Sincerely,

Marie-Laure Denis

The Chair