CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The President

[redacted]

LRAR n° 2C 137 386 0347 4

Examination of the case:
[redacted]

Paris, on December 22nd, 2021

No./Réf.: [redacted]CM214287

Case no. 21004812
(To be referenced in all correspondence)

Dear Mr. President,

This is further to the exchanges that took place between the services of the French data protection authority (Commission nationale de l'informatique et des libertés "CNIL") and the data protection officer of [redacted] company within the framework of the examination of [redacted]'s complaint, transmitted to the CNIL by the German data protection authority from Bavaria pursuant to Article 56.1 of the General Data Protection Regulation ("GDPR").

This complaint was about the security and confidentiality of booking confirmation emails sent by the [redacted] Indeed, [redacted] stated that he had booked a hotel room in [redacted] The emails confirmation of his reservation received in this respect from [redacted] on December 3rd, 7th and 8th, 2019 were passing through the server [redacted] which was not using TLS protocol.

First, in response to our electronic mail of April 1st, 2021, your company specifies that the mail server [redacted] is managed by the [redacted] company to which [redacted] has entrusted services relating notably to the sending of electronic booking confirmations. This server benefited from the standard settings recommended by your provider [redacted] Thus, it stems from your response that the TLS setting was indeed activated for the most common recipient mail servers (google, yahoo, icloud…). However, for other less common recipient servers (such as the [redacted] server used by the complainant), this setting was not activated.

On this issue, your company argues that the systematic activation of the TLS protocol for mail servers would be a practice mainly known in the banking sector. It would indeed be "*likely to affect the performance of emails reception, which can be critical in the case of booking confirmations which, in addition to being required by the regulations, are very much expected by customers who want to be reassured that their purchase is going well*". Your company adds that the absence of activation of the TLS protocol would imply attack capabilities that are not available to "mainstream" hackers and that "*if successful, the sole concerned data would be those contained in the booking confirmation, which are not of a sensitive nature*".

RÉPUBLIQUE FRANÇAISE
3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr
Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif. Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

Yet, it belongs to the processor to implement "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (...) encryption of personal data*" (Article 32.1.a GDPR).

In this case, the sender is more precisely required to ensure an end-to-end encrypted transport channel at *"the state of the art"*, and this, for an end-to-end management of its electronic shipments. He must therefore guarantee an encrypted transport channel between its sending server ([redacted]) and all recipients servers, such as the one here ([redacted]). Indeed, the transmission of personal data through public networks shall be subject to security measures enabling to ensure its confidentiality and integrity. Therefore, the implementation of a protocol, such as the TLS protocol, enabling the encryption and authentication of data appears necessary in such context.

Therefore, by not providing an encrypted transport channel when sending the booking confirmation which included [redacted]'s personal data, [redacted] has failed to comply with its security and confidentiality obligations provided under Article 32.1 of the GDPR.

However, I note that your company has of its own doing activated the TLS protocol on April 23rd, 2021 systematically in order to test the possible impact on performance. After a monitoring period, in the absence of regressions compared to the previous configuration, your company decided to keep this setting for sending its electronic communications. All sendings from the [redacted] server are now carried out with the activated TLS protocol (screenshot provided in support).

In this respect, I would like to remind you that in order to guarantee in an optimal way the security of exchanged data, the TLS protocol must be associated with cryptographic chains that have no known vulnerabilities. That is why its version 1.3, which only offers state-of-the-art cryptographic algorithms, should be privileged. For all intents and purposes, the French Agency for the Security of Information Systems (ANSSI) has published several security recommendations for the TLS protocol in its note version 1.2 of 03/26/2020, available at the following URL : https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/.

The answers provided by your company, and in particular the measures taken by the latter, lead me, in agreement with other European data protection authorities concerned by the processing, **to proceed to the closure of this complaint**.

Yours Sincerely,

[redacted]