

The President

Registered letter with AR

N°: 2C137409/1426A



Paris, on

02 NOV. 2021

Our Ref.: [REDACTED]RAL211042

Cases n° 19011346, n° 19016027, n° 19016065
(to be referenced in all correspondence)

Dear Sir,

This is further to the exchanges that took place between the CNIL's services and [REDACTED], then Data Protection Officer (DPO) of [REDACTED], in the framework of a first complaint which has been transmitted to us by the data protection authority of Rhineland-Palatinate (Germany), according to provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

This complaint (case n° 19011346) was lodged by [REDACTED] a German customer of [REDACTED] who had noticed several security flaws concerning the processing of personal data linked to your term deposit activity.

Two other complaints relating to the same facts and the same processing were subsequently transmitted to us by the data protection authority of Rhineland-Palatinate concerning other German customers, [REDACTED] (case n° 19016027) and [REDACTED] (case n° 19016065).

The complainants state that they received unencrypted or weakly encrypted e-mails confirming the opening of term deposit accounts, making their name, address, account number and the amount deposited easily accessible.

The exchanges that have taken place between the CNIL departments and the [REDACTED] DPO lead me, in agreement with the other European data protection authorities concerned by the data processing, to reprimand [REDACTED] in accordance with the provisions of Article 58.2.b) of the GDPR.

Indeed, I would remind you that, as a data controller, it is your responsibility to ensure the security and privacy of the personal data you process, by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk (**Article 32 of the GDPR**).

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

In the present case, given the sensitive nature of the information sent by unencrypted or weakly encrypted e-mail (i.e. names, first names, addresses, account numbers and amounts deposited), illegitimate access to these data by malicious third parties may entail a risk for the data subjects (in particular, attempts at extortion from third parties who may know the address and amount deposited at the time of the opening of the term account). Therefore, it appears necessary to communicate these data via a secure communication channel.

Yet, following the first exchange between the CNIL and your services, the security flaw reported by the complainants was confirmed. Corrective measures were taken to remedy this situation by increasing the level of security in the processing of the personal data of customers with fixed-term deposit accounts.

However, these first corrective measures (isolation of personal data in a separate document protected by a password) did not provide adequate protection insofar as the encryption of documents containing clients' personal data was too weak and thus made documents easily accessible by a third party.

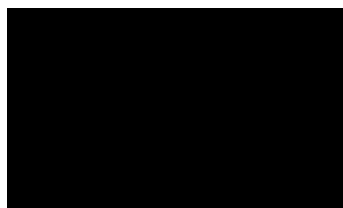
Nevertheless, I note that this problem has since been corrected: the email acknowledging receipt of the subscription documents no longer contains any personal data. Subsequent communications containing personal data of your customers are now sent by post.

I also take note of the establishment of a customer area (Online Banking) effective since October 20, 2020 allowing secure access to personal messaging (without storage of documentation).

I therefore note that [REDACTED] has brought the processing of the personal data of its customers implicated by these three complaints into conformity by taking the appropriate technical and organisational measures to remedy the security and confidentiality defects identified.

Finally, I would like to point out that this decision, which closes the examination of the aforementioned complaints, does not preclude the CNIL from using, in the event of new complaints, all the other powers conferred to it under the law of January 6th, 1978 as amended and the GDPR.

Yours sincerely,



Copy to [REDACTED] Data Protection Officer

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