

The Deputy Vice-President

[REDACTED]
MADAME THE DIRECTORATE GENERAL
[REDACTED]

Paris, the

Our ref: [REDACTED]

References to be recalled in all correspondence

Registered letter with acknowledgement of receipt N°XXXXXXX

Dear Director-General,

The company [REDACTED] manages in particular the [REDACTED], which provides banking, savings, insurance and credit products to individuals and professionals. The majority of [REDACTED]'s clients are resident in France and a few in other EU countries.

In accordance with my **decision N°2024-108C of 27 March 2024**, the Commission Nationale de l'Informatique et des Libertés (CNIL) carried out an inspection on 12 June 2024 at the premises of the company [REDACTED].

This control is part of a “*coordinated enforcement framework*” of the European Data Protection Board (EDPB) which decided, in 2024, to verify the conditions under which public and private bodies manage the exercise of the right of access.

The findings made during that inspection, as well as the additional information provided on 24 June and 9 December 2024, lead me to note the following facts.

I. Analysis of the facts at issue

Failure to comply with the obligation to respect the right of access

In law, Article 12(2) of the GDPR provides that “*The controller shall facilitate the exercise of data subject rights under Articles 15 to 22*”.

Article 15 of the GDPR provides that every person has the right to know whether a controller holds personal data concerning him or her and lists the information to be communicated to him or her, where applicable, when exercising his or her right of access.

Recital 63 of the GDPR states that *“Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.”*

The Council of State has ruled, for the application of these provisions, that *“restrictions on access may be imposed where, in particular, requests are submitted in a non-precise manner in view of the amount of personal data processed by a file”* (EC, 5 December 2024, No 488201).

In that regard, the European Data Protection Board’s Guidelines 01/2022 on the rights of data subjects of 28 March 2023¹ state that, as a matter of principle, data subjects have the right to obtain full disclosure of all data concerning them, but that a restriction of access to part of the information may sometimes be considered.

This will be the case where the data subject has explicitly limited his or her request to a subset of processing operations or where the controller *“may have doubts as to whether a request for access, expressed in very general terms, is actually intended to receive detailed information on all types of data processed or on all branches of activity of the controller”* [...] *“In any event, the controller should always be able to demonstrate that the way in which the request is processed is intended to give the widest effect to the right of access and that it complies with its obligation to facilitate the exercise of the rights of data subjects (Article 12(2) GDPR). Subject to those principles, the controller may wait for the response of the data subject before providing additional data in accordance with the data subject’s wishes, if the controller has provided him or her with a clear overview of all processing operations that may relate to the data subject, in particular those that the data subject may not have expected, if the controller has also provided access to all data that the data subject has clearly desired and if, in addition, that information has been combined with a clear indication of how to access the other parts of the data processed”*.

In this case, the delegation was informed that, in the event of a request for a right of access, the Customer Relations Department compiles files which are specifically produced to respond to requests for access. It has been clarified that communications between the applicant and the bank, such as the history of exchanges with the Customer Relations Department, are not transmitted.

██████████ stated that it had chosen to limit the information it provides because of the large number of information systems and applications hosting its customers’ personal data.

I note that the examples of responses to broadly formulated requests for access provided to the delegation of control do not inform the data subjects that certain data have not been communicated, nor of the possibility of obtaining the communication of those data at the specific request of the person.

It follows from the foregoing that, although the response to broadly worded requests for the right of access may, by way of exception, not be exhaustive in the light, in particular, of the amount of data processed by the company, the response given to the person must clearly show the omission of certain elements and the right of the data subject to specify his or her request in order to obtain communication of those elements, which is not the case here.

Therefore, I consider that ██████████ infringed the provisions of Article 15 of the GDPR, as clarified by recital 63 of the GDPR.

¹ https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_en

II. Corrective measure ordered by the CNIL (Article 20 of the Law of 6 January 1978)

In view of those factors, and in agreement with the other data protection authorities concerned by that processing, the following corrective measure must therefore be taken against [REDACTED]

- **A REPRIMAND**, in accordance with the provisions of Article 20 of the Law of 6 January 1978 as regards the obligation to comply with the requirements in the processing of requests for right of access laid down in Article 15 of the GDPR, in particular by informing individuals where the answers provided are not exhaustive and of their possibility of obtaining communication of the omitted data.

This decision entails the closure of procedure N°2024-108C. However, this closure is without prejudice to the right reserved by the CNIL to carry out a new verification mission to verify that your company has adopted the measures required following this decision.

In the event of a new verification procedure, if your company has not complied with this measure, 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 Council of State within two months of its notification.

The CNIL's departments ([REDACTED] Legal Officer in the Inspections Department [REDACTED]) are at your disposal for any further information you may require.

Sincerely,

Sophie Lambremon
The Deputy Vice-President

Copy sent by email to [REDACTED] [REDACTED] [REDACTED] Data Protection Officer