

**DATA PROTECTION POLICY OF OPEN BANK, S.A.
AND OPEN DIGITAL SERVICES, S.L.**

1. Who is the Data Controller for my data?

Depending on the Bank subject to your complaint, the controlling Bank may be:

OPEN BANK S.A. with Tax ID number: A-28021079

Plaza de Santa Bárbara 2, 28004 Madrid.

Contact email address of the Data Protection Officer: openprivacy@gruposantander.es

or

OPEN DIGITAL SERVICES, S.L. with Tax ID number: B-87745733

Plaza de Santa Bárbara 2, 28004 Madrid.

Contact email address of the Data Protection Officer: openprivacy@gruposantander.es

2. What data do we collect about you?

The following types of data will be collected within the complaint framework:

- First and last name(s) of the people involved in the complaint and their position.
- Details, if supplied, of the whistleblower (first and last name, position, telephone number and email address).
- The events reported suspected of being criminal or improper.
- The events provided in supporting documentation required to investigate the conduct reported.

In this regard, the personal data provided for the purpose of the complaint and, in general, any processing carried out in Canal Abierto (hereinafter referred to as “Open Channel” or the “Channel”) shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, in Organic Law 3/2018 of 5 December, on Personal Data Protection and guarantee of digital rights, for legitimate and specific purposes in connection with the investigation that may arise as a result of the complaint made. It will not be used for incompatible purposes and will be appropriate, relevant and limited in relation to the aforementioned purposes.

No personal data that is not clearly relevant to the processing of specific information will be collected or, if it is collected by accident, it will be deleted without undue delay.

When the complaint is made verbally, the conversation conducted via an in-person meeting will be documented through minutes that must be confirmed by both parties.

If it is evidenced that the information provided or part thereof is untrue, it will be immediately deleted from the time of such circumstance being evidenced.

In the event that such untruthfulness could constitute a criminal offence, the information will be kept for the necessary period during which the judicial proceedings are conducted.

3. For what purpose does Openbank process my personal data and what is the legitimate basis for this?

At Openbank, we will process your data for the purpose of managing, analysing and resolving reported complaints.

The legitimate basis for processing the management of complaints will be as follows:

- If the complaints refer to contraventions of European Union law; as well as the commission of crimes or serious or very serious administrative violations or any violations of the anti-money laundering regulations or specific provisions expressly establishing the obligation to maintain a complaints channel, the legal basis of the processing will be compliance with legal obligations.
- If the complaints refer to any other violations of the applicable legal system, as well as inappropriate practices related to accounting or auditing, internal control or undue influence on external auditors (SOX), the legal basis of the processing will be fulfilment of a matter of public interest.
- With respect to complaints regarding conduct contrary to the corporate behaviour or leadership principles, the legal basis for the processing will be the legitimate interest of the bank to which the complaint refers in ensuring that the corporate behaviours, which are expected by all employees, are respected. However, data processing within this framework may not involve any imbalance to the rights of the data subjects and the processing may not cause harm to them.

If the processing of special categories of data that are necessary for the management of received complaints and its corresponding processing procedures occur, it will be considered authorised by the provisions of Article 9.2 (g) of the GDPR for reasons of essential public interest, on any of the aforementioned legal bases.

4. How long will Openbank keep my data for?

The personal data provided will be processed for the period necessary to decide on the appropriateness of initiating an investigation on the events reported, that is, within a maximum period of three months from receipt of the complaint, except in especially complex cases. Such cases may be extended for an additional three months.

After the aforementioned period has elapsed without initiating investigative actions, the data will be deleted from the reporting system, except in order to anonymously keep system

operation evidence.

In the case of non-submitted reports, these will be kept on an anonymous basis and personal data will be completely removed.

The Bank will have a log of received complaints and conducted internal investigations, thus performing diligent and thorough follow-up with the goal of maintaining traceability on the Channel's activity and providing evidence of its operation. However, in all cases, the confidentiality requirements set forth in this procedure will be guaranteed. Complaints that have not proceeded will only be kept on an anonymous basis.

5. Who could Openbank share your information with?

With regard to the sharing of data, you are expressly notified that the personal information of whistleblowers will in all cases be reserved and that it will not be shared with the persons to whom the related events refer or to third parties.

However, personal data may be shared, when necessary for the investigation or implementation of disciplinary or corrective measures, with the Santander Group bank where the reported events occurred.

Likewise, for the processing of judicial proceedings that, where appropriate, are being conducted or in those cases in which it is legally required, personal data may be shared with supervisory bodies, courts and tribunals as a result of the investigation, which may be referred to the Public Prosecutor's Office as well as to public institutions, when the proceedings fall under their jurisdiction.

The Channel is managed by Openbank, who will take all the necessary technical and organisational measures to protect the security of the data collected in order to protect it from unauthorised disclosure or access. Specifically, the Bank will ensure that the data is not disclosed to the investigated party during the investigation and will always respect the fundamental rights of the person, without prejudice to any actions that may be taken by the competent judicial authorities.

Openbank, within the service provision framework, has the Ethicspoint platform from the provider NAVEX. In this regard, the Bank follows strict selection criteria for service providers in order to comply with its data protection obligations and formalises the corresponding data processing agreement with them. Thus, appropriate safeguards have been implemented to ensure respect for the independence, confidentiality, data protection and the secrecy of reports.

6. International data transfer

The Channel platform and consequently all processed personal data are stored and hosted in the European Economic Area. However, the sub-processors include NAVEX Group companies that may carry out international transfers of personal data in a timely manner within the service support framework, in accordance with the applicable regulations:

- NAVEX personnel, as data processor, are located in the United Kingdom, a country that has been declared as having an adequate level of protection for the purposes of Article 45 of the GDPR by the European Commission, through the Decision of 28 June 2011.
- NAVEX uses sub-processors that can carry out processing activities, within the support tasks framework, from the United States. In addition, depending on the language in which the events are reported, additional sub-processors may be used to provide interpretation or translation services. The Bank will only transfer personal data to third countries by means of the Standard Contractual Clauses of the European Commission of 4 June 2021 as a guarantee mechanism recognised by the GDPR with the aim of conserving the security of data that may be subject to an international transfer. Alternatively, other suitable guarantees provided by applicable regulations may be used, depending on the destination country, including additional measures and guarantees to ensure a level of protection substantially equivalent to that provided in the European Union.

The interested party may request additional information on such appropriate guarantees through the contact means indicated in the following “Exercising rights” section.

7. Who is the data protection officer and how can I contact them?

The Data Protection Officer is in charge of protecting your privacy and confidentiality, as well as guaranteeing compliance with the different legal requirements contained in the regulations (both Spanish and European) related to personal data protection.

You can contact our DPO by emailing us at: openprivacy@gruposantander.com

8. What are my rights when I provide my data?

You have and can exercise the following rights:

- Right of access
- Right to portability
- Right to rectification
- Right to erasure
- Right to object
- Right to restriction of processing
- Right to not be subject to solely automated decisions

You may exercise the aforementioned rights by sending a written and signed message to the following address openprivacy@gruposantander.com attaching the DNI (National ID

number) or official document proving your identity.

Finally, you may file a complaint to ODS and/or the Spanish Data Protection Agency (as the competent Supervisory Authority for data protection), especially when you are not satisfied with the exercising of your rights, by writing to the address above, or through the website www.aepd.es.