OPEN DIGITAL
Services

# PROCEDURE USE AND OPERATION OF THE CANAL ABIERTO

## OPEN DIGITAL SERVICES, S.L.

Grupo Santander

**TABLE OF CONTENTS**

# 1 INTRODUCTION

## 1.1 Objectives

This procedure regulates the use and operation of the ODS Canal Abierto, in accordance with applicable legislation and regulations. This document should be read together with the ODS General Code of Conduct, the Canal Abierto Policy, the Canal Abierto Management Guide and the Internal Research Guide.

## 1.2 Definition and scope

Open Digital Services, S.L. (hereinafter "ODS" or "the Entity") makes available to employees, directors, members of the administrative bodies and third parties (among others, suppliers and customers) with which it has a relationship, to report alleged non-compliance referred to in paragraph 1.2. Of the Canal Abierto Policy and in Annex I of this procedure, together with the definitions that will be considered for the interpretation of this procedure.

## 1.3 Scope of application and transposition in subsidiaries

This procedure is elaborated and approved by ODS using the procedure for the use and operation of the Canal Abierto of the parent entity as a reference document incorporating the adaptations that have been considered necessary. It has direct effectiveness in ODS and is fully applicable in its scope.

# 2 DETAIL OF THE COMMUNICATION MANAGEMENT PROCESS THROUGH THE CANAL ABIERTO

The process of use and operation of the Canal Abierto has the following phases:

## 2.1 Sending and receiving communications

Communication through the Canal Abierto may be carried out by one of the following means, which are managed by a provider external to the Group:

- Through the EthicsPoint platform managed by an external provider through the following link:

  ods.ethicspoint.com

- Calling by phone to the number that is published on the Canal Abierto platform
- Likewise, a letter may be sent to the fulfillment function of the parent entity to the following postal address:

  Regulatory compliance

  Plaza de Santa Bárbara, 2, Edificio R, entreplanta

  28004-Madrid

Likewise, you can request a face-to-face meeting with the managers of the Canal Abierto, to which two people from that team will attend and that will take place within a maximum period of seven days from the request made by the informant.

Annex II also lists some of the channels established by external bodies for the communication of conduct considered to constitute serious or very serious criminal or administrative offenses or infringements of European Union law.

If the communication received is not anonymous, the identity of the informant will be reserved in any case and the necessary measures will be taken to preserve confidentiality and the information subject to the communication and the rights of the informant.

When the communication is made verbally, the informant will be warned that it will be recorded or transcribed and will be informed of the processing of their data in accordance with the applicable regulations. Without prejudice to the rights that correspond to him in accordance with the data protection regulations, the informant will be offered the opportunity to review the transcription to verify, rectify and accept by signing the content.

If a communication object of the Canal Abierto is received by a person other than those responsible for the management of the same, said person must keep absolute confidentiality of the information received and send the communication immediately to those responsible for Canal Abierto.

Communications made through this Canal must collect the following information in order to facilitate the assignment for processing, investigation and management to the corresponding team:

- Identification of the informant when the communication is chosen in a confidential and non-anonymous manner. For this purpose, the name and surname and email address must be indicated.
- Identification of the person to whom the facts are reported, if any.
- Description of the events reported, indicating (if possible) the dates on which they took place; and
- Elements on which the suspicion of irregularities is based.

Once the communication has been received, regardless of the means used (face-to-face meeting, through the platform, by telephone or by post), it will be registered on the Canal Abierto, you will be assigned an identification code and registered on the EthicsPoint platform securely and with restricted access to authorized people.

### 2.2 Admission to procedure

The regulatory compliance function of the parent entity will be the one who receives the communications and makes a preliminary evaluation of them in order to verify that they are within the scope of application of the Canal Abierto, in accordance with paragraph 1.2 of the Canal Abierto Policy, and will send an acknowledgment of receipt to the informant within a maximum period of 5 calendar days.

Once the preliminary analysis has been carried out, it will be decided by the person responsible for the management of the Canal, within a period that may not exceed five working days from the date of entry to the Canal Abierto of the communication, whether it is accepted for processing or not, informing, if appropriate, the informant within three working days of the decision date, unless the communication is anonymous or the informant has waived receiving communications about the communication made.

For clarification purposes, communications that refer to:

- Facts that do not refer to any of the matters expressed in section 1.2 of the Canal Abierto Policy and 1.2 of this procedure or only contain personal opinions or subjective assessments outside the purpose of this Channel
- Communications describing facts or circumstances that are manifestly unfounded or plausible.
- Communications that do not provide new information about previous ones
- Communications that reveal reasonable evidence that information has been obtained through the commission of an offense. In this case, in addition to the inadmissibility, communication shall be sent to the Legal Adviser so that it may notify the Fiscal Ministry of a detailed account of the facts considered to constitute an offense, unless the analysis of that concludes the lack of typicity of the conduct.

In these cases, communication will be archived, leaving a reasonable record of this decision in the Canal Abierto register.

The disclosure decision will not prevent the further initiation of an investigation if additional information is received in accordance with the Canal Abierto Policy.

In cases in which communications involving a commercial claim are received by these third parties, the regulatory compliance function will duly inform the informant that this is not the appropriate channel, and that it may send its communication to the competent function as appropriate. To do this, the contact details of the corresponding department will be identified to resolve your request. In addition, your communication will be sent to the competent function as appropriate (customer service, the function of Financiero, etc.).

**2.3 In charge of the investigation**

If the communication is accepted for processing, the regulatory compliance function of the parent entity will refer it to the functions responsible for the investigation, which will be the following:

- Where the communication relates to breaches of legal obligations relating to equal opportunities, respect for people, reconciliation of work and personal life, prevention of occupational risks or collective rights, it shall be referred to the role of People & Culture[1] , who will be responsible for carrying out the investigation and proposing the resolution that is appropriate and measures that it deems appropriate, in compliance with the provisions of the Collective Agreement or the applicable regulations.
- When communications relate to conduct not aligned with Santander Group corporate behaviours or the ODS leadership principles, they will also be referred to the People & Culture function, in order to be responsible for the investigation, management and resolution of these cases.
- In the case of communications relating to money laundering and terrorist financing (BC/FT), sanctions, as well as bribery and corruption, shall be referred to the Financial Crime Prevention Function (FCC) of the parent entity, being responsible for the investigation, with the assistance of People & Culture if such communications affect employees.

  The communications received and related to matters not covered in the above points, will be managed by the regulatory compliance function, with the assistance of People & Culture if the facts affect employees.

In addition, in view of the case in question, the functions of Legal Adviser, Internal Audit and T&O (among others, Cybersecurity), will provide the collaboration that is deemed necessary during the investigation of the incidents received. If the role of People & Culture, Compliance or FCC is affected by the content of the communication, the investigation shall be attributed to the Legal Adviser in the Party affecting the function affected by the conflict.

Likewise, it is recommended to involve Internal Audit when the reported aspects may have a relevant impact on the unit's governance, internal control and risk management systems, which should be considered by the Investigator.

In view of the specificity of the case in question, an external adviser may be requested.

In those cases where, due to the complexity or gravity of the facts communicated or because they affect several of the matters listed above, an investigation team composed of representatives of all or some of the functions mentioned in the preceding paragraphs may be set up, led by a coordinator of the regulatory compliance function, who will be the person in charge of the investigation and directly responsible for the researchers, as well as ensuring the correct management and implementation of all the actions that must

[1] References to People & Culture throughout the present shall be understood to be made, where appropriate, in collaboration with Industrial Relations.

be carried out within the framework of the investigation. In any case, the participation of a representative of the Legal Counsel will be required when the procedure affects a member of the ODS Board of Directors.

### 2.4 Research

The investigation will include all actions aimed at verifying the veracity of the facts reported in the communication received and whether they constitute any of the breaches provided for in paragraph 1.2 of the Canal Abierto Policy and in paragraph 1.2 of this procedure.

a. Interview the person investigated

Whenever appropriate, an interview will be conducted with the person under investigation, in which he or she will be invited to present his or her version of the reported facts and to provide any evidence that he or she considers appropriate and relevant. This interview will always be carried out by the person in charge of the investigation, except in those cases that refer to minor breaches of corporate behaviour.

In this interview, the person under investigation will be informed of the facts attributed to him succinctly, without revealing the identity of the informant or giving access to the communication, so that he can argue what he considers appropriate to defend himself, in accordance with the guarantees of paragraph 2.8. of this procedure.

To document the interview, the possibility of recording it will be offered, for which the authorization of the interviewee will be required. If it is not recorded, a written record will be made indicating the attendees, matters treated and conclusions that will be shared with the respondent for review and conformity, at that time or by email.

b. Access to electronic devices

When it is necessary to access the electronic devices of employees, it will be made in accordance with the Internal Policy on Cybersecurity Standards for the protection of Santander, as well as in the Guide on Digital Rights in the workplace.

Access to the information contained in the electronic devices of the employees, owned by Santander Group, will guarantee the right to privacy of the employee, respecting the legality, equality, proportionality and privacy of the employees, collecting only information that is strictly necessary and relevant to the successful conclusion of the investigation.

### 2.5 Outcome of the investigation and measures taken

The internal investigations must be completed within 60 days, which may be extended only for justified reasons in cases of special complexity for another 30 additional days, informing the person responsible for the management of the Canal Abierto.

Once the investigation has been completed, the regulatory compliance function or the function of People & Culture, as appropriate, shall resolve the file by stating in a report the result achieved and indicating in any case:

- An account of the facts reported in the communication
- The actions carried out in order to verify the veracity of such facts
- The conclusions reached in the research

In any event, the report will focus on the facts gathered during the investigation, avoiding expressions or conclusions based on personal opinions.

To ensure the confidentiality of the investigation, the report will be shared only under the premise of "*need to know*" to people entitled to know the facts investigated or who have a role in making decisions regarding the outcome of the investigation.

The report shall include, in line with paragraph 2.2 of the Policy:

- A proposal for a decision to discontinue communication without acting due to lack of substantiation of the communication or the failure to verify the responsibility of the person under investigation; this shall be notified to the informant and, where appropriate, to the person concerned.

  In this case, the informant will be entitled to the protection provided for in the Canal Abierto Policy and in this procedure.

- A proposal to assess measures, if communication is well founded, in accordance with the provisions of the Canal Abierto Policy.

  The function of People & Culture, in coordination with the Labor Relations function, shall decide, in accordance with its disciplinary authority and in compliance with the labour regulations in force established in the collective agreement, the corresponding measure and proceed to its execution, or propose its adoption to the competent bodies in the case of the most serious situations.

  In addition, other non-disciplinary measures may be taken, such as *coaching*, training, awareness-raising sessions or any other measures deemed appropriate by the People & Culture team.

  Exceptionally, when the gravity of the matter so requires, the function of People & Culture may apply the precautionary measure of suspension of employment, always respecting the time limits provided for in the applicable labour regulations.

  The person responsible for managing the Canal Abierto shall forward the file to the Legal Adviser when it considers that it may be appropriate to pursue legal actions or, where appropriate, to send the communication to the authority, entity or body that considers itself competent for processing, it includes the Public Prosecutor's Office, when the facts could be inadvertently constituting a crime or the European Public Prosecutor's Office in the event that the facts affect the financial interests of the European Union.

In any case, the Legal Adviser will proceed to the immediate referral to the Fiscal Ministry without the need to complete the investigation when the person responsible for the Canal Abierto, on the proposal of the investigating team, it transmit the file to the investigating team because it considers that rational evidence of the commission of a potential offense has been revealed, unless the analysis by the investigating team concludes the atypical nature of the conduct.

Once the investigation is completed, and in view of the facts reported and the conclusions reached, the investigator reserves the right to modify the taxonomy proposed by the informant, so that it conforms to the definitions, for errors in the cataloging by the informant.

## 2.6 Monitoring of breaches of the Code of Conduct

The purpose of this section is to establish the process that guarantees adequate oversight by the governing bodies of the implementation and application of the Code of Conduct on ODS by reporting non-compliance with the Code of Conduct and its implementing regulations to the Executive Committee ODS and the ODS IT, Cyber, Risk & Compliance Committee within their respective competences.

This process addresses the following points:

- Means of identifying breaches of the Code of Conduct
- Inventory of breaches of the Code of Conduct and Taxonomy for classification
- Stakeholders and their roles and responsibilities in the process
- Relationship with other internal ODS processes Means of identifying breaches of the Code of Conduct:

Non-compliance with the Codes of Conduct and its development policies shall be identified through the following means:

- Canal Abierto
- Communications made by ODS employees to their People & Culture managers.
- Breaches detected by control areas and reported to People & Culture managers for appropriate disciplinary action.
- Results of internal audits in which specific breaches of the Code of Conduct are reported and managed by People & Culture officials.
- Controls carried out by the different ODS areas (Cybersecurity, Costs etc.) within the framework of their ordinary activity that are raised by People & Culture managers for their management and sanction, if appropriate, in a disciplinary process.
- Non-compliance detected by People & Culture managers in the framework of their activity.

Inventory of breaches of the Code of Conduct and Taxonomy for classification:

Based on the above means of identification, potential and actual breaches of the Code of Conduct will be collected in a single inventory at the local level, which will include breaches collected in the field of the parent entity and the ODS. This inventory shall be reported to the governing bodies of the parent entity and ODS at least once a year so that, within the scope of their functions, they may supervise the proper implementation of the Code of Conduct at the local level. In this single inventory, the classification of breaches of the Code of Conduct will be made considering by Compliance and Labor Relations the taxonomy established in the Canal Abierto Policy.

The single inventory of non-compliance will be reported at least annually to the ODS Executive Committee by the Governance, Risk & Compliance function, reporting holistically, consistently and comprehensively on compliance with the ODS Code of Conduct.

Stakeholders and their roles and responsibilities:

The compliance function of the parent entity and People & Culture managers shall collect the information as follows:

- The compliance function will identify as potential and actual breaches of the Code of Conduct, the cases admitted to processing and managed in the Canal Abierto in order to determine the number of communications received, the taxonomies of these cases, and the number of cases substantiated and disciplined.
- People & Culture managers will identify breaches of the Code of Conduct that have been received outside the Canal Abierto by the means indicated in the preceding paragraphs. To this end, People & Culture teams will identify as actual and potential breaches of the Code of Conduct the incidents of conduct they have managed and, where appropriate, disciplined.

Consolidation of information: In order to ensure the consistency of the information collected for the report to the governing bodies of the parent entity and ODS, People & Culture managers will submit to compliance information regarding cases of breaches of the Code of Conduct they have managed and compliance will ensure that the categorization criteria is homogeneous and consistent with that used in the Canal Abierto policy and are not stated duplications regarding the information collected through the local ethical channel.

Relationship with other processes of the Group:

The information resulting from the process of identification of breaches of the Code of Conduct serves to establish synergies that reinforce other processes of the Group by providing transparency and completeness the degree of implementation of the Code of Conduct, its development policies and compliance with corporate behaviours.

The process of identifying breaches of the Code of Conduct is interrelated with the following processes:

- Previous:

Or analysis procedure for the application of malus and clawback clauses to members of the identified collective who are disciplined for breaches of the Code of Conduct.

Or identification of trends, concentrations and action plans to mitigate possible identified risks that affect local units due to their seriousness or repetition.

- Subsequent:

Disciplinary procedure: Which allows the Executive Committee and the IT, Cyber, Risk & Compliance Committee to be informed of the analysis of the main breaches, trends and potential risks arising from the Code of Conduct.

The purpose of this section is to establish the process that guarantees adequate oversight by the governing bodies of the implementation and application of the Code of Conduct on ODS by reporting non-compliance with the Code of Conduct and its implementing regulations to the Executive Committee of ODS in the area of its competences.

The compliance function will identify as potential and actual breaches of the Code of Conduct, the cases admitted to processing and managed on the Canal Abierto in order to determine the number of communications received, the taxonomies of these cases and the number of cases substantiated and disciplined.

### 2.7 Reporting and escalation

On an annual basis, ODS Governance, Risk & Compliance will report to the IT, Cyber, Risk & Compliance Committee on the analysis of Canal Abierto metrics. To do this, it will use the information that will previously make available the compliance function of the entity head. - Exceptions are made in cases relating to money laundering and terrorist financing and/or sanctions that will be governed by current legislation and internal regulations on this matter, without prejudice to the statistical data for this type of communication.

Finally, the informant and the person under investigation will be informed, provided that such communication does not compromise the confidentiality of the informant, of the outcome of the investigation, and if applicable whether measures have been taken, considering the right of privacy of the parties involved.

If the information or communication of the person under investigation could compromise the confidentiality of the informant, all necessary measures must be taken to preserve such confidentiality and, if this is not possible, the right to confidentiality of the informant in good faith shall prevail over the right to information of the person under investigation.

In cases where the incident relates to accounting or auditing issues, in accordance with the Capital Companies Act and SOX regulations, once the investigation is completed and provided that the investigation concludes the existence of infringements in this matter, the resolution will be submitted by the regulatory compliance function of the parent entity to the Board of Directors of ODS, which will decide on the appropriate measures in this case.

The regulatory compliance function of the parent entity shall periodically inform the Board of Directors of ODS of the communications received that refer to practices or acts in the field of accounting or auditing.

The Responsible of the Canal Abierto shall inform the Head of Governance, Risk & Compliance of ODS periodically and at least once a year of the management and evolution of the Canal Abierto, so that he may report to the ODS Executive Committee.

For the purposes of the procedure for applying *malus* and *clawback* clauses and the Santander Group Remuneration Policy, the People & Culture function will be informed of communications affecting members of the identified group, once the investigation has been completed and the responsibility of the manager has been verified.

### 2.8 Guarantees and rights of the informant and the person investigated during the management of the communication

The guarantees and rights of the people involved in communication shall be those provided for in section 2.2. and 2.3 of the Canal Abierto policy.

### 2.9 Mechanisms to prevent conflicts of interest

In addition, the following mechanisms have been established to prevent possible conflicts of interest:

- Reception of communications through an external online platform that ensures the integrity of communications and the traceability of access by the research team.
- Receiving communications is limited to a control function. The regulatory compliance function of the parent entity receives all communications through the Canal Abierto. Who in turn will transfer or involve the relevant area in accordance with paragraph 2.3.
- Identification and profiling of people who have access to the communication management platform related to the Canal Abierto.
- Existence of a mechanism whereby the tool identifies communications involving a person in the regulatory compliance function of the parent entity with the power to process and investigate communications received through the Canal Abierto; they will be sent directly to the Head of the Canal Abierto for research and management.
- Assignment to the investigation to functions not affected by a conflict of interest arising from the content of the communication, when, in the opinion of any of the functions involved in the communication, another is affected by that conflict. In the event of a dispute between them, and if the latter does not resolve by agreement of the people responsible for each of them, the matter shall be settled by a third function.

### 2.10 Processing of communications from the point of view of data protection

Only the following types of data may be collected in the context of communication:

- Name and surname of the people involved in the communication and their position.
- Information about the informant (name and surname, title, telephone number and email address) in case the informant decides to identify himself.
- Alleged criminal or irregular acts reported.
- How much supporting documentation is required to investigate the reported conduct.

In this sense, the personal data provided for the purpose of the communication will be treated in accordance with the applicable data protection regulations, for legitimate and specific purposes in relation to the research that may arise as a result of the communication made, they will not be used for incompatible purposes and will be adequate, relevant and limited in relation to the aforementioned purposes.

Once the reasons for the incident and the absence of bad faith have been established, and the measures have been taken to prevent the confidentiality of the informant from being compromised, the person who has been the subject of the communication shall be informed, complying with the provisions of Article 11 of Organic Law 3/2018, of 5 December, of Protection of Personal Data and Guarantee of Digital Rights, on the fact of which he is accused, as well as how to exercise their rights in accordance with data protection regulations, unless such communication relates to issues related to the prevention of money laundering and terrorist financing and/or sanctions, in which case the provisions of Law 10/2010 will apply, 28 April and implementing regulations, prevention of money laundering and financing of terrorism and specific sanctions regulations. And finally, the person who has been the subject of communication will be informed of the estimated deadline for the processing of the communication. In any case, the

parent entity, as a guarantee of confidentiality to the informant, confirms that in general the exercise of the rights of the person under investigation could be limited by the particularity of the communication and may only be exercised on the personal data subject to treatment. In no case may the data relating to the information be included within the exercise of the rights by the person under investigation.

If it is not possible to adopt measures to safeguard the confidentiality of the informant in the event of communication to the person under investigation, the right of the former shall prevail in accordance with the provisions of article 31.2 of Law 2/2023, of 20 February, regulator of the protection of people reporting on regulatory offenses and the fight against corruption.

If there is a risk that the notification may compromise the investigation, it may be deferred until the said risk disappears. In any event, the period for informing the person under investigation shall not exceed one month from the date of registration of the communication, unless the person under investigation is not properly and/or sufficiently identified or if the initial communication to the person under investigation could jeopardize the successful completion of the investigation of the communication file, in which case, such communication may be deferred until the danger disappears, not being able to exceed said postponement of the term of sixty (60) calendar days from the submission of the communication.

The foregoing shall not apply to communications that do not correspond to the objective scope of the Canal Abierto or that are not substantiated or to those corresponding to cases of money laundering and terrorist financing and/or sanctions that will be governed by current legislation and regulations applicable domestic law

On the other hand, in addition to the entity to which the person investigated and/or informant belongs, the personal data contained in the facts communicated may be transferred to supervisory bodies, courts and tribunals as a result of the investigation that may be launched, there is the possibility that the informant can be summoned judicially.

The parent entity will ensure that it adopts all the technical and organizational measures necessary to preserve the security of the data collected in order to protect them from unauthorized disclosures or access. In particular, the parent entity has adopted appropriate measures to guarantee the confidentiality of all data and will ensure that the data are not disclosed to the person under investigation during the investigation, respecting in all cases the fundamental rights of the person, without prejudice to actions that, where appropriate, they may be adopted by the competent judicial authorities.

Personal data relating to communications received and internal investigations shall only be retained for as long as it is necessary and proportionate for the purpose of complying with applicable law. In no case may the data be kept for a period exceeding 10 years.

The regulatory compliance function of the parent entity carries out an anonymization of the communications received on the Canal Abierto, keeping the personal data in force 3 months from the closing of the communication on the EthicsPoint platform, if required, according to the applicable regulation

The interested party may at any time exercise the rights of access, rectification, erasure, limitation of processing and opposition, as well as any other that he or she has recognized by the applicable data protection regulation. To do so or to consult any question regarding the processing of your personal data, you can send an email to openprivacy@gruposantander.es or, by postal mail, to Plaza de Santa Bárbara 2, 28004, Madrid (A/A. Data Protection Officer/Privacy Office - Compliance).

## 3 RESOLUTION OF CONSULTATIONS AND TRAINING ON THE USE OF THE CANAL ABIERTO

The regulatory compliance function of the parent entity shall be responsible for resolving inquiries received from employees regarding the use and operation of the Canal Abierto and, where appropriate, for developing and supervising, in coordination with the function of People & Culture, training and awareness plans regarding the use and operation of the Canal Abierto by employees.

## 4 OWNERSHIP, INTERPRETATION, VALIDITY DATE AND REVISION

### 4.1 Ownership of the proceedings

The development of this procedure is the responsibility of ODS Governance, Risk & Compliance

Its initial approval, as well as any revisions from the date of approval to be made in this document, will be carried out by the ODS Executive Committee.

### 4.2 Interpretation

It is up to the ODS Governance, Risk & Compliance function to interpret this procedure.

In case of conflict between the Spanish version and the English version, the Spanish version will always prevail.

### 4.3 Date of validity and review of the policy

This procedure shall enter into force from the date of its publication. Its content will be subject to periodic review, making changes or modifications.

## 5 VERSION CONTROL

| ID | Incumbent | Maintenance | Validation | Approval | Date |
|---|---|---|---|---|---|
| 1 | Governance, Risk & Compliance ODS function | Governance, Risk & Compliance function & ODS | IT, Cyber, Risk & Compliance and Compliance Committee Function of the parent entity | ODS Executive Committee | 03/12/2025 |

| ID | Comments |
|---|---|
| 1 | First version of the procedure for the use and operation of the Canal Abierto (adaptation to ODS of the Canal Abierto procedure of Openbank and ODS) |

**ANNEX I: TYPE OF CASES THAT CAN BE REPORTED THROUGH THE CANAL ABIERTO AND DEFINITIONS**

| Category | Subcategory | Definition |
|---|---|---|
| **General of Code Conduct** | **Marketing of products and services** | To market products or services without fulfilling the obligation to treat the client fairly, acting with honesty, impartiality and professionalism. |
| | **Conflicts interest/activities outside ODS** | Situations in which the personal or financial interests of an employee - or those of his or her immediate family members or anyone with whom the employee has a significant relationship - interfere in some way with his or her ability to serve the best interests of ODS, its clients, and/or other interest groups. |
| | **Gifts and invitations** | When a professional abuses his duties in Santander by offering, delivering, promising, requesting or accepting any type of gift, benefit/consideration or invitation to obtain a personal advantage for him or a third party, affecting his impartiality. |
| | **Corruption, and bribery bribery** | An act of corruption can arise when an individual abuses his position of power or responsibility for his own personal benefit.<br>Bribery acts that give someone the financial or other advantage to encourage that person to perform his or her duties or activities improperly or to reward that person for having already performed it. This would include attempting to influence a decision-maker by granting some kind of additional benefit to the decision-maker, beyond what can be legitimately offered.<br>Bribery as a bribery involving both a national and international public official. |

| | | |
|---|---|---|
| | **Prevention of Money Laundering and Terrorism Financing and Sanctions** | Money-laundering is (i) the conversion or transfer of property, knowing that such property is derived from criminal activity or involvement in criminal activity; for the purpose of concealing or concealing the illicit origin of property or assisting people involved in avoiding the legal consequences of their acts; (ii) The concealment or concealment of the nature, origin, location, disposition, movement or actual ownership of property or rights in property, knowing that such property is derived from criminal activity or involvement in criminal activity; (iii) the acquisition, possession or use of property, knowing, at the time of receipt, that it originates from criminal activity or from involvement in criminal activity; (iv) Participation in any of the activities referred to in the preceding paragraphs, association to commit such acts, |
| | | attempts to commit such acts and the act of aiding, instigating or counseling someone to carry out them out or facilitate their execution. |
| | **Corporate Defense** | Conduct that prevents, restricts or distorts free and effective competition to the detriment of the market, of ODS clients (who are other entities of the Santander Group) and of all those with whom commercial and / or professional relations are maintained. Some of these behaviors are the exchange of sensitive information with competitors, price agreements, market sharing, bid manipulation or tender. |
| | **Privacy/Information Security/Information Confidentiality** | Privacy and protection of information imply refraining from disseminating information to third parties, for example, personal information of customers, employees (salaries, permits, etc.), security/strategic information of Santander, as well as information related to the entities with which Santander maintains commercial relations. These obligations are maintained even after termination of employment and the use of confidential information for financial gain is prohibited. |
| | **Internal fraud** | Fraud attempted or perpetrated by one or more internal parties against the organization, i.e. an employee or a subsidiary of the organization, including cases where an employee acts in collusion without external parties. |

| | | |
|---|---|---|
| | **Cybersecurity** | Cybersecurity risks include: i) unauthorized access to or misuse of information or systems (e.g., theft of personal information, merger and acquisition plans or intellectual property); ii) financial fraud and theft (e.g., diversion of payments, withdrawal of funds from<br>customers, credit card fraud, identity theft, etc.); (iii) disruption of business activity (e.g., sabotage, extortion, denial of service). |
| | **Equal opportunities and nondiscrimination** | Behaviors that are not aligned with the basic principle of action in ODS regarding providing equal opportunities in access to work and career advancement, ensuring at all times the absence of discrimination based on sex or sexual orientation, race, religion, disability, origin, origin, origin, etc. civil status, age or social status. |
| | **Sexual or sex-based harassment** | Disrespectful behavior or unwanted sexual behavior that is annoying and generates an intimidating, offensive or hostile environment at work. |
| | **Workplace harassment** | Systematically hostile or abusive treatment in the workplace that causes an intimidating, offensive or hostile environment. |

| | | |
|---|---|---|
| **Fraud** | **External fraud** | The type of fraud attempted or perpetrated by an external party(s) against the organization or clients with responsibility of the entity. There may be cases where an internal party is also involved in fraud. |
| **Accounting and Audit** | **Accounting and auditing** | Alteration or falsification of financial information, inaccuracies in financial statements, intentional misrepresentation of information, undue influence on auditors, questionable practices in accounting, auditing or internal financial controls. |
| **Labor issues and non-compliance with corporate behaviors** | **Non-compliance with corporate behaviors** | Non-professional conduct by co-workers or managers who are not aligned with Santander Way's corporate behaviors. |
| | **Serious disrespect** | Conduct involving serious disrespect by co-workers or managers in the work environment. |
| | **Non-compliance with labor regulations** | Any failure to comply with the regulations (legal or conventional), policies or internal procedures of ODS that imply the breach of a labor obligation as well as those categorized in the current collective agreement. |
| | **Failure to comply with ODS leadership principles** | Non-professional behaviors by employees that are not aligned with ODS leadership principles. |
| **Others** | Any breach of current legal or internal regulations and of ODS policies or procedures in relation to functional or organizational aspects not mentioned in the above categories. | |

**ANNEX II: EXTERNAL CHANNELS FOR REPORTING OFFENSES COVERED BY THE MATERIAL SCOPE OF APPLICATION OF LAW 2/2023**

- **Channel established by the Independent Authority for the Protection of the Informant**
- **Banco de España:** https://www.bde.es/bde/es/secciones/sobreelbanco/Transparencia/Informacion_inst/registro-deacti/Canal_de_denuncias.html
- **National Commission for Markets and Competition (CNMC):** https://sede.cnmc.gob.es/tramites/competencia/denuncia-de-conducta-prohibida

- **National Securities Markets Commission (CNMV):** https://www.cnmv.es/portal/whistleblowing/presentacion.aspx#:~:text=Escribiendo%20a%3A%20Comunicaci%C3%B 3n%20de%20Infracciones,revelar%20su%20identidad%20o%20no
- **SEPBLAC:** https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio/