Appendix to the Management Board's resolution no. 208/2024 dated
11 of October 2024

INTERNAL REPORTING PROCEDURE (WHISTLEBLOWER PROTECTION)

Santander Bank Polska S.A.

TABLE OF CONTENTS

1 INTRODUCTION

1.1. Purpose and context

This *Procedure* specifies the rules for reporting violations of the law and taking follow-up actions based on the Whistleblower Protection Act[1], also taking into account the corporate standards applicable in the Santander Group[2] and the Santander Bank Polska Group[3]. This *Procedure* is the only and comprehensive regulation specifying the rules for reporting and taking follow-up actions within the scope regulated by the aforementioned Act.

1.2. Scope of application in subsidiaries

The Internal Reporting Procedure (whistleblowers protection) applies directly to Santander Bank Polska S.A and it is approved in line with the *Procedure for the management of compliance regulations*.

The *Internal Reporting Procedure (whistleblowers protection)* should be adopted or its provisions should be incorporated into the regulations of the following subsidiaries of the Bank:

1) Santander Factoring sp. z o.o.,
2) Santander Leasing S.A.,
3) Santander Towarzystwo Funduszy Inwestycyjnych S.A.,

Subsidiaries are expected to use this document as reference when establishing their own regulations. They should generally reflect the solutions presented in this Procedure in their internal regulations, but their more specific solutions may differ from the ones used by the Bank.

2 DEFINITIONS AND KEY PRINCIPLES

2.1. Subject matter of internal reports

The subject of an internal report may be a breach as: an act or omission that is unlawful or intended to circumvent the law and involves:

1) corruption;
2) public procurement;
3) services, products and financial markets;
4) prevention of money laundering and terrorism financing;
5) products' safety and compliance with relevant requirements;

[1] Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws of 2024, item 928)

[2] **Santander Group:** a group of companies comprising Banco Santander S.A. as parent entity and companies controlled, directly or indirectly, by Banco Santander S.A. For the avoidance of doubt, the Santander Group consists of Banco Santander S.A. as parent entity, as well as entities and subsidiaries of the Santander Group.

[3] **Santander Bank Polska Group, hereinafter referred to as the Group:** a group whose parent company, within the meaning of the Accounting Act of 29 September 2009, is Santander Bank Polska S.A., hereinafter referred to as the **Bank.**

6) security of transport;
7) preservation and protection of the environment;
8) radiological protection and nuclear safety;
9) food and feed safety;
10) animal health and well-being;
11) public health;
12) consumer protection;
13) protection of privacy and personal data;
14) ITC and network security;
15) financial interests of the European Union, Poland's State Treasury or local government units;
16) EU's internal market regulations, including those concerning competition, state aid and corporate taxation;
17) constitutional freedoms and rights of man and citizen – arising in the relationship between the individual and public authorities and not related to the areas indicated in points 1-16.

2.2. Whistleblower

The person authorised to report cases under this *Procedure* is a whistleblower, i.e. a natural person who reports information about an breaches detected in in the context of their work-related activities. A whistleblower may be:

1) an employee;
2) a temporary employee;
3) a person working under a civil law contract or other arrangement that is not a form of employment relationship;
4) an entrepreneur;
5) a commercial proxy;
6) a partner or shareholder/member;
7) a member of the decision-making body for a legal person or an organisational unit without legal personality;
8) a person who performs work under the supervision and direction of a contractor, sub-contractor or supplier;
9) an intern;
10) a volunteer;
11) a trainee.

The *Procedure* also applies to the person indicated above if the internal reporting of an breach detected in the context of their work-related activities was made prior to establishment of an employment relationship or any other legal arrangement for the performance of work or services or for performance of functions in the Bank or for the benefit of the Bank; or already after the termination of such relationship or arrangement.

2.3. Other definitions

1) follow-up action – an action taken to assess the veracity of the information presented in the internal report and to counteract the reported breach (in particular through: an investigation, initiation of an inspection or other legal proceedings) or to close the case;

2) retaliatory action – a direct or indirect act or failure to take action that occurs in work-related circumstances as a result of an internal report and that violates (or is likely to violate) the whistleblower's rights or causes (or is likely to cause) undue harm to the whistleblower, including the unwarranted initiation of proceedings against the whistleblower;

3) information about the breach – information, including reasonable suspicion, about an actual or potential breach that has occurred or is likely to occur at the Bank or information concerning an attempt to conceal such an breach;

4) feedback – information about follow-up actions planned or taken and the rationale for such actions, provided to the whistleblower;

5) context of work-related activities – past, present or future actions taken in connection with the work carried out under an employment relationship or any other legal arrangement for the performance of work, services or functions in the Bank as part of which the whistleblower has detected the breach or might become subject to retaliation actions;

6) person reported – a natural person, a legal person or an organisational unit that is not a legal person but but has legal capacity under applicable laws; presented in the internal report as the infringer or as a person with whom the infringer is associated;

7) whistleblower's aide – a person who helps the whistleblower make the internal report in the context of their work-related activities and whose assistance should not be disclosed;

8) person connected with the whistleblower – a natural person who may suffer a retaliation action, including a co-worker or immediate family member/partner within the meaning of Art. 115 (11) of the Criminal Code Act of 6 June 1997 (Journal of Laws of 2024, item 17)[4];

9) internal report, also known as report – notification of a breach to the Bank;

10) external report – oral information or a written notice about breach, provided to the Commissioner for Human Rights or a public authority.

[4] i.e. a spouse, ascendant, descendant, sibling, relative by marriage in the same line or degree, a person in an adoptive relationship and his or her spouse, as well as a person living in cohabitation.

2.4. Basic principles

1) The *Procedure* applies to a whistleblower who makes an internal report in the context of their work-related activities, irrespective of the legal relationship serving as the legal grounds for performance of work.
2) The internal report may be filed anonymously or non-anonymously.
3) A whistleblower is protected under the *Procedure* from the moment they make the report – provided that they had reasonable grounds to believe that the reported information was true at the time it was disclosed and that it referred to the actual breach.
4) The said protection does not apply to a whistleblower who intentionally makes an internal report knowing that no breach has occurred (bad faith).
5) Actions provided by law may be taken against persons found to have committed a breach, including actions under the labour law and internal regulations (in particular: *Work Regulations* or the *General Code of Conduct*.) In accordance with the Work Regulations, decisions on disciplinary measures are taken by the whistleblower's line manager in cooperation with the HR unit.
6) Under the Whistleblower Protection Act, a whistleblower may also make an external report. External reports are filed with the Commissioner for Human Rights or other public authority who are competent to take appropriate follow-up action with respect to the problem reported.[5] Where appropriate, external reports are filed with EU institutions, authorities or offices/agencies. All information on making external reports (together with a links to the websites of the public authorities accepting such reports) is presented on the Bank's website under the tab "Investor Relations – Corporate documents".

3 PROCEDURES FOR INTERNAL REPORTING AND FOLLOW-UP

3.1. How to file internal reports

1) The Bank's Management Board has authorised the dedicated members (hereinafter referred to as the authorised) of the compliance unit to receive internal reports and initiate follow-up actions, including verification of the internal report and further communication with the whistleblower (such as asking the whistleblower and the Bank's other organisational units for additional information or providing substantive support, or providing feedback to the whistleblower) and to maintain the register of internal reports.
2) A breach can be reported through the following internal reporting channels:
    a. **via email to sygnalista@santander.pl,**

[5]As regards external reporting, the Whistleblowers Protection Act comes into force on 25 December 2024.

b. via the **dedicated app** indicated on the Bank's website ("Investor relations – Corporate documents" tab) and intranet – from the date of its physical launch and publication on the Bank's website and intranet
c. **via regular mail** sent to the Bank's compliance unit at following address:
Komórka ds. zgodności, ul. Kolorowa 10, 60-198 Poznań, with a note: "ETYKA - POUFNE",
d. **via regular mail** sent to the Management Board member in charge of the Compliance and FCC Division to the following address:
al. Jana Pawła II 17; 00-854 Warszawa, with a note "DO RĄK WŁASNYCH - ETYKA - POUFNE".

3) Reports concerning the president or member of the Management Board should be filed with the Chairman of the Supervisory Board via regular mail sent to:
al. Jana Pawła II 17; 00-854 Warszawa, with a not note "DO RĄK WŁASNYCH - ETYKA - POUFNE".

4) At the request of the whistleblower, the internal report may be made also during the meeting. At the meeting, there should be two representatives of the compliance unit authorised to receive internal reports, and the meeting should be arranged within seven days from the date of receipt of such a request.

5) In order to verify the internal report diligently and take effective follow-up actions, the internal report should include at least:
   a) personal data of the whistleblower (in the case of non-anonymous reports),
   b) data of the person concerned ,
   c) contact address of the whistleblower (mailing address or e-mail address),
   d) the subject of the breach and its description, including a citation of any circumstances that may be relevant to the proper consideration of the application,
   e) work context that enabled identification of the breach,
   f) reasonable grounds for claiming that the information about the breach is true.

3.2. Receiving internal reports

1) The report concerning the employee of the compliance unit, including authorised to receiving internal reports, is escalated for further processing to the employee relations unit. The employee relations unit forwards information about the receipt of the report to the member of the Management Board in charge of the Compliance and Financial Crime Prevention Division (CCO).

2) An authorised employee of the compliance unit who receives the report reads it and finds whether the report contains: specific/ sufficiently detailed information enabling follow-up activities with respect to the reported breach or consults the contents of the report with a relevant unit being a subject-matter expert with respect to the contents of the report, and then takes follow-up actions independently or with substantive support of a relevant unit.

3) When the Chairman of the Supervisory Board receives the report, after an initial verification, he/ she sends it to the Management Board member in charge of the Compliance and FCC Division

(CCO), keeping it confidential, unless a conflict of interest arises. The report may be provided in a confidential manner through an authorised employee handling the matter of the Supervisory Board.

4) When the Management Board member in charge of the Compliance and FCC Division (CCO) receives the report, after an initial verification, he/ she appoints an employee or a unit responsible for verifying of the breach and taking follow-up actions, in particular obtaining substantive support (allowing for the possibility of sending the case to other specialist units).

5) When the report concerning the CEO of the Management Board or the Management Board member is sent via the internal reporting channels indicated in it. 3.1. 2) a-c to the compliance unit e mployee, the report will be sent to the Chairman of the Supervisory Board to decide on further actions.

6) If the report is made orally during the meeting with authorised employees of the compliance unit, it may be documented with the consent of the whistleblower in the form of:
    a. a recording of the conversation in a durable and retrievable form, or
    b. a complete and accurate minutes of the conversation prepared by an authorised employee of the compliance unit (the whistleblower can check, correct and approve the minutes by signing it).

7) The Bank's employee authorised to receive internal reports, conducts a preliminary verification of the report to check whether it meets the conditions specified in this *Procedure* (in particular whether the report falls within the subject and personal scope of *Procedure*, is work-related and has reasonable grounds). If the internal report needs to be clarified or additional information needs to be provided, the employee contacts the whistleblower, if he gave a contact address.

8) If the internal report meets the conditions referred to in item 7) and the contents of the internal report are reasonable enough o instigate investigation, an authorised employee of the Bank
    a) takes explanatory actions,
    b) in 7 days as of receipt of the report sends to the whistleblower the confirmation of receiving the report and starting to consider it, unless the whistleblower has not provided the address to which the confirmation could be sent.

9) Internal reports that cannot be reviewed without the whistleblower completing or explaining the information contained therein may be closed after 15 days of a documented attempt to obtain additional information (and classified as "insufficient information" to consider the case). The reporting person will be informed about the closure of the case and the reason for it closure, provided that the whistleblower provided the contact data.

10) The Bank can refrain from reviewing the report that has been reported previously by the same or different whistleblower, if that report does not contain new information about the breach that would be material for the case when compared to the previous report. The employee authorised

to receive the reports informs the whistleblower that the internal report has not been reviewed, and the reason for such decision.

11) If the report made via internal whistleblowing channels does not concern the breach of the law referred to in item 2.1. or when the report is made by a person who is not a whistleblower within the meaning of item 2.2., or the report concerning the Bank's subsidiary, the application will not be explained and will be subject to consideration in the manner specified in this *Procedure*. As appropriate, the reporting person will receive information about the possibility of reporting the matter independently to another appropriate channel in the Bank or the Group (if they have provided a contact address).

12) In the case referred to in point 11, with the consent of the reporting person, it may be forwarded to the appropriate channel for reporting breaches by the Compliance Unit.

13) Lack of consent referred to in point 12 does not exclude the Bank's right to take other explanatory or preventive actions in connection with the information received about the breach/potential breach, while maintaining the confidentiality standards regulated by this *Procedure*.

14) If the report meeting the provisions of this *Procedure* is made in other channels available at the Bank, the report can be sent internally to the appropriate channels indicated in this *Procedure*.

3.3. Follow-up actions

1) Every internal report submitted, sent or made orally is be recorded in the register of internal reports.

2) Subject to the case described in point 3.2.1., follow-up action in connection with a report shall be undertaken by a designated employee of the compliance unit referred to in point 3.1.1.

3) As part of the follow-up actions taken, the compliance unit employee may use the substantive support of employees of other Bank units competent with respect to the subject of the report, including requesting their addition to the team conducting the explanatory proceedings. The compliance unit employee may delegate specific activities to other members of the Team as part of the follow-up actions taken.

4) Employees who are not members of the compliance unit may join the investigation team only if approved by the Head of the Compliance Monitoring Department, unless a a service level agreement (SLA) has been signed between the compliance unit and the other organisational unit involved.

5) Depending on the nature of the case, such employees are selected by the delegated member of the compliance unit in line with need-to-know principle and in consideration of potential conflicts of interest as well as subject-matter skills of these other organisational units, in particular:
   a) financial fraud – financial crime prevention unit,

b) accounting frauds and financial statement-related frauds – the finance unit;
c) corruption and prevention of money laundering and terrorist financing – AML unit;
d) cybersecurity – cybersecurity unit;
e) market abuse – market abuse-prevention unit
f) practices in restraint of trade – legal unit
g) privacy protection /information security/confidentiality of information – dedicated unit for information security/ personal data protection.

6) The composition of the Team may be supplemented at any stage of the case if it is necessary for its proper consideration.

7) Persons conducting the investigation have the option request additional information from such other persons/units, at each stage of the process.

8) At the request of the person conducting the investigation, the head of the Bank's unit asked to provide support in the investigation process is obliged to appoint a person from their unit to join the team or provide the requested information.

9) If in the course of the investigation, circumstances arise that may distort objectivity or lead to the conflict of interests of people making up the investigation team, then these persons should instantly disclose the fact to other team members and (to a limited extent) their line managers and refrain from participating in the investigation going forward.
Depending on the nature of disclosed circumstances and availability of other employees to handle the investigation, the CCO may take the following decisions to address the arising conflicts of interest:

- appoint new members to join the investigation team;
- extend their personal oversight of the pending investigation;
- remove certain persons from the investigation team
- using the support of an external expert in the follow-up actions taken.

For detailed rules on the management of the conflict of interest, please see the *Conflict of Interest Prevention Policy of Santander Bank Polska S.A.*

10) The investigation team may access the information related to the internal report on the need-to-know basis, i.e. as necessary for the proper verification of the said report (available information limited to the purpose and content of the report).

11) Team members and any person requested by the investigation team to provide internal report-related information are obliged to keep in confidence the whistleblower's and case details both during the investigation and after it has been finalised. Maintaining confidentiality with regard to a person means protecting the confidentiality of the identity of the whistleblower, the person concerned by the report, and the third party indicated in the report.

12) Regardless of the right to delegate specific activities to other members of the Team, authorized employee of the compliance unit supervises the conduct of the explanatory proceedings - unless the investigation concerns an internal report filed with respect to that very employee.
The monitoring covers:
    a) confirmation of receipt of the report to the whistleblower and providing feedback to the whistleblower on time,
    b) notifying the person concerned about the receipt of the report and the results of the proceedings,
    c) investigation documents (whether complete), indicating:
        - the list of investigation team members (persons or organisational units) and the list of persons/units requested to provide information for the purpose of investigation;
        - the list of persons who have been notified of the investigation results in a non-anonymised form (in justified cases).

13) The delegated employee of the compliance unit or other members of the investigation team notify the person concerned (whilst observing all confidentiality rules and without revealing the identity of the whistleblower) that the internal report has been filed and relevant investigation has been commenced – within 15 working days of the report-receipt-confirmation date[6]. However, this time limit may be extended if such a notice to the person concerned might have a negative impact on the course of the ongoing investigation.

14) If transfering the information about the report to the person concerned or conducting investigations with their participation could result in revealing the identity of the whistleblower, all necessary measures should be taken to protect their identity. In the event that this proves impossible, the right of the whistleblower not to reveal their identity will take precedence over the right of the person concerned to receive information about the case. Persons conducting the proceedings are obliged to inform the whistleblower of any case where the anonymous nature of the report or failure to reveal their identity to the person concerned may limit the possibility of fully investigating the case. However, the decision to reveal their identity always rests with the reporting person.

15) In the course of the investigation, the person making the internal report and the person concerned have the right to be heard, to present their arguments and evidence and to name witnesses in the case.

16) Upon a prior consent of the individuals engaged in the investigation, electronic devices can be used to record the interviews which constitute part of the meeting/interview. If the participant in the proceedings does not agree that the interview be recorded or the form of interview does not guarantee the confidentiality of the recording (while the interview must be recorded), then the

[6]The above-mentioned time limit is determined by the need to complete the information/documents from the reporting person and to verify them for the purpose of investigation.

participant in the proceedings will answer the questions in writing during or immediately after the interview.

17) At each stage of the investigation, the participants may be asked for further statements or clarifications. The participant's refusal to provide such information may result in his or her perspective not being taken into account in the final conclusions.

18) Members of the investigation team have access to internal report-related information only to the extent required to verify such report.

19) The cases are investigated without any delay; however, with consideration given to the time required for due investigation of the case.

20) If the investigation is still in progress after 60 days after the said confirmation date, then the whistleblower should be notified accordingly and informed about the new time limit for the investigation, unless the whistleblower did not provide a contact address to which the feedback should be sent. The investigation may be extended by max. 3 months after the internal report receipt confirmation date or – if no such confirmation has been given – by 3 months after the lapse of 7 days from the internal report date.

21) Investigation is documented with a written report or a file note.

22) The designated employee of the compliance unit shall provide the whistleblower with feedback within a period not exceeding 3 months from the date of being informed of the receipt of the report - unless the whistleblower failed to provide a contact address to which the feedback should be forwarded.

23) Investigation may be suspended for the period when whistleblower or the person concerned is on sick leave or other absence, provided that their presence is necessary to analyse the circumstances of the case - however, this does not affect the time limit for providing feedback to the whistleblower, as referred to in point 22. In this case, the feedback includes information on the further follow-up actions taken so far and planned. The investigation is not suspended in the situation which poses a threat to the employees' health or with regards to suspected crimes.

24) The authorized employee of the compliance unit notify the person concerned about;
    a) the outcome of the investigation (negative verification of the internal report rationale)– immediately after the investigation has been completed, via email and (if required and feasible) in person,
    b) the outcome of the investigation (positive verification of the internal report rationale) – within 3 business days from completion of the investigation procedure, via email and (if required and feasible) in person,
    c) processing of personal data – at the first contact, at the latest within one month of obtaining the data.

25) Investigation results may also be provided to other persons, with the knowledge of the director of the Compliance Monitoring Department, (unless it affects the confidentiality or anonymity of the internal report), in particular to:
   a) the manager of the person who filed the internal report (at the consent of that reporting person);
   b) the manager of the person who has been reported;
   c) the member of the Management Board of the division where the person concerned works, and if the investigation involves a person employed outside of the divisional structure – to the President of the Management Board;
   d) the President of the Management Board – if the person concerned is a member of the Management Board and the reported breach has been confirmed;
   e) the Chairman of the Supervisory Board – if the person concerned is the president or member of the Management Board or head of the Internal Audit Area and the reported breach has been confirmed;

26) In special circumstances, investigation results may also be provided to other persons than the above mentioned (unless it affects the confidentiality or anonymity of the internal report), at the consent of the director of the Compliance Monitoring Department.

27) If the internal report has been made to the Management Board member in charge of the Compliance and FCC Division or Chairman of the Supervisory Board, then these persons are informed about completion of the investigation and (if necessary) about the ensuing findings. They may also receive updates when the investigation procedure is still in progress (if need be).

28) If the results of the explanatory proceedings in a given case indicate grounds for initiating other legal proceedings (e.g. criminal, civil, administrative), the designated employee of the compliance unit forwards appropriate information on this subject to the persons or units of the Bank responsible for initiating or conducting such proceedings.

29) The investigation may be ended with recommendations concerning appropriate remedial measures aimed to:
   - mitigate the legal, regulatory and reputation risks for the Bank;
   - prevent any similar breaches going forward.

30) In the case of proceedings ending up with recommendations, compliance unit employee/the investigation team can verify whether the recommended remedial measures have been implemented.

31) Irrespective of the recommendations above, after completion of the investigation, disciplinary measures may be taken against the person proved to have committed the breach – as per item 2.4.5) of the *Procedure*.

32) It is forbidden to put pressure or perform any other unacceptable actions against the individuals or team concluding the investigation to influence their findings or proposed conclusions or recommendations. Any such attempt must be reported to the CCO.

4 PROHIBITION OF RETALIATION AND PROTECTIVE MEASURES

1) No retaliation or attempts of threats of retaliation can be taken against the whistleblower. No retaliatory action of a punitive nature may be taken against persons reporting a matter in good faith as a result of the report made. It is prohibited to take any retaliatory action, including threatening to take such action, against the reporting person or to draw any other consequences for reporting an action or conduct that is suspected of violating the law.

2) The retaliation actions include in particular:
   a) refusal to engage in an employment relationship;
   b) termination of an employment relationship with or without notice;
   c) failure to enter into an employment contract for a definite period or an employment contract for an indefinite period after termination of the employment contract for a probation period – if the whistleblower had a legitimate expectation that such an agreement would be concluded with him,;
   d) failure to enter into another employment contract for a definite period – if the whistleblower had a legitimate expectation that such an agreement would be concluded with him,;
   e) failure to convert an employment contract for a definite period into an employment contract for an indefinite period, where the whistleblower had legitimate expectations that he or she would be offered permanent employment;
   f) reduction in wages;
   g) withholding of promotion or being overlooked for a promotion;
   h) being overlooked for work-related benefits other than remuneration or having the amount of those benefits reduced;
   i) demotion;
   j) suspension from employment or professional duties;
   k) transfer of the whistleblower's duties to another employee;
   l) unfavourable change of location of place of work or working hours;
   m) a negative performance rating or employment reference;
   n) imposition or administering of any disciplinary measure, including a financial penalty or a similar measure;
   o) coercion, intimidation or ostracism;
   p) harassment;
   q) discrimination;
   r) disadvantageous or unfair treatment;
   s) withholding of participation in training or being overlooked for selection for an professional qualifications training;

t) unjustified medical referrals, including psychiatric referrals;
u) actions aimed at making it more difficult for the whistleblower to find a job in a particular sector on the basis of a sector or industry-wide informal or formal agreement;
v) causing a financial loss, including loss of business or loss of income;
w) non-material harm, including to the whistleblower's moral rights, and in particular their reputation.

3) The prohibited retaliation measures include also early termination, termination without notice or cancellation of a contract to which the whistleblower is a party, in particular a contract for goods or services.

4) Retaliation is also prohibited against persons helping the whistleblower in filing the report, persons connected with whistleblowers, and also legal persons or other organisational units helping the whistleblower or connected with the whistleblower, in particular those owned by the whistleblower or hiring the whistleblower.

5 INTERNAL REPORTS REGISTER

1) The compliance unit runs an internal reports record with all reports sent to the internal reporting channels. That register can be part of a register used for storing reports other than internal reports withing the meaning of the Internal Reporting Procedure, but it must be possible to separate it from the register in a way that prevents unauthorized persons from accessing the register.

2) The register contains:
   a) report reference number,
   b) subject of the breach,
   c) personal data of the reporting person and the person concerned required for their identification – unless they have not been provided in the report,
   d) contact data of the reporting person – unless they have not been provided in the report,
   e) date of the report,
   f) information on follow-up actions taken,
   g) case closure date.

3) The register can also contain other data required for reporting and analysis of trends in reporting.

4) Personal data in the internal reporting register are kept for 3 years after the end of the calendar year in which the follow-up actions have been taken with respect to a given report, or after the end of the proceedings initiated with the follow-up actions.

6 INFORMATION SECURITY

6.1. Personal data protection

1) Personal data is processed only to the extent necessary to accept the report or to take any necessary follow-up action. Personal data that is not relevant to the processing of the report is not collected, and in the event of accidental collection, it is immediately deleted. The deletion of such personal data takes place within 14 days from the moment it is determined that it is not relevant to the case.

2) The Bank may process personal data related to explanatory proceedings pursuant to Article 6(1)(c) and Article 6 (1)(a) of the GDPR, with respect to disclosure of the whistleblower's data. Detailed data categories may be processed based on Article 9 (2)(g) of the GDPR.

3) The personal data of the reporting person and other personally identifiable information cannot be disclosed, except with express consent of that person or when the person making the report had no reasonable grounds to believe that the information that was the subject of the report was true at the time of reporting and that it constituted information about a violation of the law.

4) Personal data processed in connection with receipt of the report or in the internal reporting register are kept for 3 years after the end of the calendar year in which the follow-up actions have been taken with respect to a given report, or after the end of the proceedings initiated with the follow-up actions.

5) In any non-standard cases, the investigation team consults the scope, legal basis and data retention period with the Personal Data Protection Office.

6.2. Anonymity and confidentiality rules

1) Confidentiality protection applies to information based on which the identity of the reporting person, person concerned and third parties indicated in the report may be directly or indirectly established.

2) It is ensured that the identity of the reporting person is not disclosed to anyone beyond the authorised employees competent to receive or follow up on reports, without the explicit consent of that person. This applies also to any other information based on which the identity of the reporting person may be directly or indirectly established.

3) The investigation team is subject to confidentiality at each stage of the process and after its completion. This obligation consists, among others, in:
   a) limiting the number of persons required for examining the case,
   b) holding conversations related to the investigation in separate rooms,
   c) encrypting documents,
   d) applying the confidentiality clause in any related correspondence,

e) parties to the investigation and testifying individuals are instructed about their confidentiality obligation;
f) documents are recorded on electronic devices or in systems with access strictly limited to the individuals authorised to conduct the investigation,
g) data storage devices, including recorded conversations, are destroyed after the expiry of the storage period, pursuant to the principles of personal data protection.

4) The confidentiality and anonymity of the individual who had reported the case and of individuals asking to remain anonymous is kept throughout the investigation and after its completion.

5) The Bank will take no actions aimed at identifying the whistleblower.

6) Only persons holding written authorisations of the Bank may be allowed to accept and verify reports, take actions as part of the explanatory proceedings and process personal data of persons referred to in section 1.

7) The authorised persons are obliged to keep secret the personal data and information that they obtained while receiving and verifying reports and taking actions under explanatory proceedings, also after termination of their employment relationship or another legal relationship under which they performed that work.

7 OWNERSHIP AND REPORTING

1) The Bank's Management Board is responsible for adequacy and effectiveness of *Internal reporting procedure*.

2) The selected employee of the compliance unit provides quarterly updates about the results of the explanatory proceedings to the CCO.

3) The Management Board member in charge of the Compliance and FCC Division (CCO) informs the CEO of the Management Board and the Supervisory Board about relevant[7] reports at least once every six months as part of the compliance unit's periodic reports provided to the Bank's Management Board and Supervisory Board.

4) The Supervisory Board, as required, minimum once a year, assesses the adequacy and effectiveness of *Internal reporting procedure*.

[7]The following reports are considered relevant:
- reports concerning the CEO of the Management Board, members of the Management Board, chairman of the Supervisory Board, members of the Supervisory Board and Internal Audit Area director,
- reports concerning persistent, recurring or large-scale irregularities in implementation of procedures/ processes that can cause the risk of the Bank's criminal, civil law or administrative liability or expose the Bank to regulatory sanctions,
- reports that contain information that can generate high reputational risk for the Bank, Santander Bank Polska Group or Santander Group.

8 OWNERSHIP, INTERPRETATION, VALIDITY AND REVIEW DATE

- This *Procedure* is adopted after consultations with trade unions operating in the Bank pursuant to Article 24 section 3 item 1 and section 4 of the Whistleblower Protection Act.
- This *Procedure* is approved by the Management Board of Santander Bank Polska and Supervisory Board of Santander Bank Polska.
- The compliance unit is the owner of this *Procedure* and is responsible for its interpretation.
- This *Procedure* comes into effect on the date of its publication after 7 days from the date of its notification to persons working at the Bank. Its contents is subject to periodic reviews in order to introduce any changes or modifications deemed appropriate.

9 CHANGE CONTROL

Date	Version	Description	Author	Date of consultation with trade unions	Date of approval by Management Board	Date of approval by Supervisory Board
08.10.2024	1	The first version of the document resulting from implementation of the Whistleblowers Protection Act	Compliance Monitoring Department	25.09.2024-07.10.2024		