

Lead Document Manager	• Ines Cieslok	Reviewed on	• October 2024
Lead Document Owner	• Erda Cani	Implementation Date of this current version	• October 2024

Note: Further document metadata is available in the central repository/database.

1. Document Scope and Applicability

This Standard applies to SSBI as follows:

Country Perspective

SSBI Country	Covered by Standard?	Any Additional Local Standard in Place?	Deviations of Local Standard vs. SSBI Standard
Germany	Yes	No	•
Austria	Yes	No	•
France	Yes	No	•
Italy	Yes	No	•
Luxembourg	Yes	No	•
Netherlands	Yes	No	•
Poland	Yes	No	Poland Branch specific whistleblowing process is outlined in the Poland Branch Appendix
Switzerland	Yes	No	•

Business Line/Business Area/Corporate Function Perspective

Within the countries/locations indicated above, this Standard applies to staff members (including, but not limited to, board members, employees, contractors, volunteers, trainees, persons working under the supervision and direction of contractors, subcontractors and vendors) in:

- All business lines
- All areas and departments
- All corporate functions

2. Rationale and Description

Several laws require SSBI to establish channels and procedures for internal reporting and follow-up of concerns regarding potential or actual breaches of applicable laws and regulations or policies.

As a credit institution established in Germany, SSBI must implement appropriate measures that allow its employees to report concerns on potential or actual breaches of applicable laws & regulations, while maintaining the confidentiality of their identity [Section 25a (1) Sent. 6 No. 3 of the German Banking Act (Kreditwesengesetz – KWG)].

Also the local implementing laws of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (**EU Whistleblowing Directive**) require the establishment of an internal reporting channel and procedures for follow-up by SSBI including its branches.

Moreover and to the extent applicable, the German Act on Corporate Due Diligence Obligations in Supply Chains (German Supply Chain Due Diligence Act) requires that enterprises in scope of this Act have an appropriate internal complaints procedure in place which enables persons to report human rights and environment-related risks as well as violations of human rights or environment-related obligations that have arisen as a result of the economic actions of enterprise in its own business area or of a direct supplier of the enterprise.

A key component of State Street's Standard of Conduct is to encourage all employees to follow a culture of speaking up, and to report concerns on potential or actual misconduct, violations of policies or applicable laws and regulations.

Without prejudice to the external reporting channels to the competent authorities, employees can report internally their concerns directly to their manager/next level manager, Compliance, the Conduct Risk Management team (ethics@statestreet.com), Global Security, Corporate Audit, Global Human Resources or Legal. Once a report has been made internally, the relevant management team should complete a report (on behalf of the reporter) via the Speak Up Line, to ensure that the proper investigation team and resources are allocated to review the matter.

State Street operates the Speak Up Line via an independent third party vendor, which is a confidential third-party resource where State Street employees or external third parties (i.e. contingent workers, former employees, job applicants, clients and vendors) can raise any concerns including matters that may fall under the scope of the EU Whistleblowing Directive as implemented by local whistleblowing legislation (**Whistleblowing Matter**). This document shall provide additional details on:

1. How employees can report concerns internally using the Speak Up Line and/or externally to the competent authorities in the relevant jurisdiction; and
2. the roles and responsibilities around reviewing, investigating, reporting and decision making on the Speak Up Line cases and Whistleblowing Matters concerning SSBI.

ESG and CER considerations

- Not applicable

3. Standard Statements

3.1. How to report a concern internally using the Speak Up Line (Internal Reporting)

The Speak Up Line is active for 24 hours a day, 365 days a year and is available in several languages.

Staff have the following options to report a concern about potential or actual misconduct, policy violations or breaches of laws and regulations via the Speak Up Line. The Speak Up Line is also available for external parties like clients or vendors. Please also consult the Speak Up Line FAQ's, the most updated version is available under this [link](#).

Report a concern online via a web-form using the following link:

<https://secure.ethicspoint.com/domain/media/en/gui/55139/index.html>

Report a concern via a dedicated telephone line:

Country	Speak Up Line – Telephone Details
Germany	0800 182 0469
Austria	0-800-200-288 At the English prompt dial 888-736-9833
France	0800-91-2790
Italy	800-761-628
Luxembourg	800-26-172
Netherlands	0800 020 1867
Poland	0-0-800-111-1730
Switzerland	0800-225-191

Reports can be made anonymously (except where not permitted by local law), although a reporting person selfidentifying may allow us to expedite the investigation as swiftly and appropriately as possible.

The reporting person receives an acknowledgement of receipt of the report within seven days following submission.

In the case of Whistleblowing Matters, the reporting person should also receive feedback from the investigating team on the follow-up of the investigation within three months of receiving the report.

For Poland Branch there is a separate Appendix that specifies the process and regulatory requirements in more detail.

3.2. External Reporting

Employees and external third parties may report an issue directly to the relevant local regulators, including but not limited to those listed in the table contained in Annexe 1.

In some jurisdictions, reporting to a regulator may not be conditional on a report first being made using internal channels. In some cases, it is possible for a reporter to report an issue using State Street's internal channels and also to a regulator and these routes may be used simultaneously or consecutively. Where a breach can be addressed effectively internally, staff are encouraged to report to internal reporting channels before reporting through external reporting channels.

3.3. Review and Investigation of Reported Matters

All reports made to the Speak Up line are treated in a confidential and sensitive manner and are only shared within State Street to the extent necessary for proper follow-up and investigation. Reports related to SSBI business and its employees will be reviewed and investigated by internal subject matter experts within the entity (including its branches, as applicable) who are qualified and appropriate to handle the matter.

In the case of Whistleblowing Matters concerning potential or actual violations of laws, regulations or State Street policies, the investigation will be led by a senior manager of the SSBI Legal, Audit and/or Compliance function, with support from the relevant corporate function subject-matter-expert(s), as required and determined by the nature of the matter.

For other matters which do not qualify as Whistleblowing Matters and as such are outside the scope of whistleblowing violations, in particular, matters relating to the treatment of people, personal grievances and/or terms of employment, such matters will be handled by SSBI Global Human Resources (GHR) Employee Relations, unless the nature of the matter or other specific circumstances suggest for an allocation of the matter to another corporate function for review and investigation (see also below “Review of Potential Conduct Violations”). .

Investigations are conducted in accordance with State Street’s global Guidelines for Conducting Internal Investigations and the relevant SSBI Addendum.

In case the investigation relates to a matter related to Anti-Money Laundering/Countering the Financing of Terrorism, the respective entity Money Laundering Reporting Officer needs to be informed accordingly.

In course of the investigation, the Investigation Leader, assisted by SSBI GHR Employee Relations, where required, shall act as an impartial person and will maintain communication with the reporting person.

Regardless of whether the Reports have been qualified as a Whistleblowing Matters or not, if the case investigated has a nexus with SSBI GmbH – Italy Branch (“SSBI Italy”), it must be immediately escalated to the local Head of Global Human Resources of SSBI Italy who will consult with local Compliance and Audit Functions to evaluate potential implications with Italian Legislative Decree 231/01 perspective (criminal liability of companies). In case the item escalated triggers the requirements for being considered a breach of the Italian Legislative Decree 231/01, the Organismo di Vigilanza (231/01 Committee) of SSBI Italy will be immediately notified.

3.4. Review of Potential Conduct Violations

When the Investigation Leader, assisted by SSBI GHR Employee Relations, where required, identifies a potential conduct violation, they will, in accordance with any applicable guidelines or procedures:

- report these potential conduct violations to the SSBI Head of Compliance and SSBI Head of Legal and seek advice, where required,
- confirm whether there has been a conduct violation,
- report any confirmed conduct violation to the Conduct Standards Committee in such form as the Conduct Standards Committee may determine.

3.5. Conduct Standards Committee

To ensure confirmed conduct violations are treated in a consistent manner across State Street, the Conduct Standards Committee (CSC) evaluates alleged conduct violations, and recommends the conduct level and sanctions, if there has been a violation.

The Conducts Standard Committee is supported by the Conduct Working Group where SSBI is represented.

3.6. Decision Making Post-Investigation

Upon completion of the investigation, the Investigation Leader will summarize the findings and recommendations for follow-up action to SSBI Management for decision-making.

The responsible Investigation Leader ensures that feedback is provided to the reporting person within a reasonable timeframe, not exceeding three months from the acknowledgement of receipt for Whistleblowing Matters.

3.7. Decision on Disciplinary Measures and Sanctions

In case of a confirmed conduct violation, the Investigation Leader, assisted by SSBI GHR Employee Relations, will present the recommendation to SSBI Management for the final decision on the disciplinary measures and sanctions to be applied. For Level II Conduct violations, the recommendation will include guidance from the Conduct Standards Committee (or Conduct Working Group, as applicable).

3.8. Protections

3.8.1. Personal data protection and confidentiality

The whole Speak Up Line process and handling of Whistleblowing Matters is subject to personal data protection regulations and requirements applicable to sensitive data. Reports and related investigation materials shall be stored by the investigating corporate function team in a secure, restricted access folder and the data retained for no longer than is necessary, proportionate and in accordance with applicable jurisdictional data retention timeframes. Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

The data shall be processed in a secure and restricted manner that ensures that the confidentiality of the identity of the reporting person and any third party mentioned in the report is protected, and prevents access thereto by non-authorised staff members.

3.8.2. Prohibition of retaliation

Retaliation against the reporting person, including threats of retaliation and attempts of retaliation, whatever the nature, are strictly prohibited in accordance with the State Street Standard of Conduct and the SSBI NonRetaliation Policy (16-P16).

4. Roles and Responsibilities

- SSBI senior manager from either the Legal, Audit and/or Compliance function is responsible for reviewing and investigating Whistleblowing Matters.
- SSBI GHR Employee Relations is responsible for reviewing and investigating (typically nonwhistleblowing) people-treatment related Speak Up Line cases concerning SSBI employees and to engage on a timely basis with SSBI Head of Compliance and SSBI Head of Legal in the case of potential/confirmed conduct matters.
- The relevant investigating corporate function lead is responsible for ensuring the provision of timely feedback to the reporting person, in accordance with applicable legal timeframes.
- SSBI Head of Compliance and SSBI Head of Legal are responsible for providing advice during the process of analysing and confirming conduct breaches.
- SSBI representative members of the Conduct Standards Committee and/or the Conduct Working Group are responsible for attending the meetings, as applicable.
- The Investigation Leader, assisted by SSBI GHR Employee Relations, is responsible for presenting the recommendation to SSBI Management for the final decision on the disciplinary measures and sanctions to be applied, including guidance from the Conduct Standards Committee (or Conduct Working Group, as applicable) for Level II Conduct violations.
- SSBI Management is responsible for making the final decision on the disciplinary measures and sanctions.

5. Key Term Definitions

Term	Definition
• Conduct Standard Framework	• A framework maintained by the Conduct Standards Committee that classifies employee conduct matters according to severity and identifies corresponding outcomes; the current framework is attached to the Conduct Standards Policy as Appendix A and may be updated from time to time by the Conduct Standards Committee. The Conduct Standards Framework and related Outcomes Framework shall be guidance only, which the CSC may deviate from for any reason, stated or not, and any resulting deviation by the CSC shall be final and binding.
Term	Definition
• Whistleblowing Matter	• matters that may fall under the scope of the EU Whistleblowing Directive as implemented by local whistleblowing legislation.

6. Annexes



20240704 - List of
EU competent authori

7. Related Policies and Standards

- Standard of Conduct; [Standard of Conduct \(sharepoint.com\)](#)
- Whistleblowing Policy - Global
- SSBI Non-Retaliation Policy (16-P16)
- SSEHG Group Guideline for Conducting Internal Investigations
- Conduct Standard Policy - Global

-----[end of document]-----

Poland Branch Appendix to Whistleblowing and Speak Up Standard**State Street Bank International GmbH Poland Branch****Document Type: Appendix****8. Document Scope and Applicability**

Poland Branch Appendix to Whistleblowing and Speak Up Standard SSBI (the: “Appendix”) is established by State Street Bank International GmbH Spółka z ograniczoną odpowiedzialnością Branch in Poland (the: “**Branch**”) pursuant to Article 24 and subsequent of the Act of 14 June 2024 on protection of whistleblowers (the: “**Act**”).

The Appendix pertains exclusively to matters related to Whistleblowing reports as specified in Article 3 of the Act on the Protection of Persons Who Report Breaches of Law (the “Act”). All other reports should be reported in accordance with the Whistleblowing and Speak Up Standard SSBI.

Terms used in this Appendix in shall have the meaning and definition specified in the Annex.

The Branch encourages and enables submission of Reports on a Breach of Law (Whistleblowing Matters) under this Appendix by Whistleblowers (as defined in 2.2) so that the Branch can investigate on and address inappropriate conduct and take appropriate Follow-up Actions. The Appendix applies solely to Reports containing Information on a Breach of Law obtained in a Work-related Context.

A Whistleblower within the meaning of this Appendix is a natural person who reports or publicly discloses Information on a Breach of Law obtained in a Work-related Context, including (without limitation): employee; temporary worker; person performing work on a basis other than employment relationship, including under a civil law contract; entrepreneur; general proxy holder; shareholder or partner; member of the governing body of a legal person or an organizational unit without legal personality; person performing work under the supervision and direction of a contractor, subcontractor, or supplier; intern; volunteer; trainee as well as a natural person referred to above in the event of reporting or publicly disclosing Information on a Breach of Law obtained in a Work-related context before the establishment of an employment relationship or other legal relationship constituting the basis for the performance of work or services or the performance of functions in a legal entity or for such entity, or the performance of service in a legal entity or even after their termination.

9. Internal Reporting

2.1 The Report may be submitted by the Whistleblower through any of the reporting channels available at the Speak Up Line operated by an independent third-party vendor, authorized by the Branch to receive the internal Reports. The Speak Up Line reporting channel is a confidential third-party resource.

2.2 The Employee Relations Director for the Branch is designated as an impartial person authorized to receive and handle Reports, including verification of a Report and further communication with the Whistleblower, in particular asking for further information and providing the Feedback. Should a Report relate to conduct of the Employee Relations Director for the Branch, such Report shall be handled by the Branch Director.

Accordingly, all Reports by Whistleblowers will be directed to the Employee Relations Director for the Branch for a plausibility check, i.e. each Report will be verified if it is subject to the Appendix and whether the Report includes sufficient and credible information, to obligatorily undertake with due diligence further Follow-up Actions, in particular to conduct an internal investigation.

10. How to report a concern internally using the Speak Up Line (Internal Reporting)

The Speak Up Line is active for 24 hours a day, 365 days a year and is available in several languages.

Whistleblowers have the following options to make a Report on a Breach of Law (Whistleblowing Matter), including a correspondence address or e-mail address (the contact address) via the Speak Up Line. The Speak Up Line is also available for external parties. Please also consult the Speak Up Line FAQ's, the most updated version is available under this [link](#).

Report a concern online via a web-form using the following link:

<https://secure.ethicspoint.com/domain/media/en/gui/55139/index.html>

Report a concern via a dedicated telephone line:

Poland - 0-0-800-111-1730

An oral report made via the Speak Up telephone line is documented in a form of a conversation protocol.

If the Whistleblower wishes to make the Report during an in-person meeting, such a meeting shall be scheduled no later than within 14 days from the date of submission of the request.

Reports can be made anonymously although a Whistleblower self-identifying may allow us to expedite the investigation as swiftly and appropriately as possible.

The Whistleblower receives an acknowledgement of receipt of the Report within seven days following submission, unless the Whistleblower has not provided a contact address.

Where a Breach of Law can be addressed effectively internally, staff are encouraged to report to internal reporting channels before reporting through external reporting channels.

11. Follow-up Actions and Investigation of the Report

All Reports made to the Speak Up Line are treated in a confidential and sensitive manner and are only shared to the extent necessary for proper Follow-up Actions.

The Follow-up Actions and in particular the investigation will be led by relevant subject matter expert(s) from Legal, Audit, Compliance or other corporate functions and coordinated by the Employee Relations Director for the Branch, as required and determined by the nature of the matter, who may collaborate in doing so with subject matter experts from relevant departments of State Street group, as it considers necessary.

In case the investigation relates to a matter related to Anti-Money Laundering/Countering the Financing of Terrorism, the respective entity Money Laundering Reporting Officer needs to be informed accordingly.

All Reports will be handled with due diligence, in a confidential manner by staff duly authorized to process personal data, in particular information revealed in course of investigation. The manager of a concerned staff member does not need to be informed, unless the investigation team considers such information may bring additional value in the investigation process.

Where Whistleblowers have identified themselves, they may be approached during the investigation, in a confidential manner, in order to provide additional information and support with the investigation process.

In all cases the investigation will be conducted in a timely (effective), impartial and professional manner.

All individuals involved in the investigation shall sign a separate undertaking regarding confidentiality.

12. Decision Making Post-Investigation (Follow-up Actions)

Upon completion of the investigation, the Investigation Leader will summarize the findings and recommendations for further Follow-up Actions (if any) in a written report to the Branch management.

The Whistleblower should receive the Feedback on the Follow-up Action within three months as of the confirmation of reception of the Report to the Whistleblower as described above or – in case the confirmation referred to above has not been provided – within three (3) months as of the lapse of seven (7) days since the reception of the Report by the Branch, provided that the Whistleblower has indicated the contact address to which the Feedback should be provided.

If the investigation concludes that the Report is substantiated, the Branch may undertake, depending on the circumstances of the given case, appropriate remediating actions, and in particular disciplinary or other legal action against the identified perpetrators of the Breach of Law or systematic actions, in compliance with the local legislation.

13. External reporting

A Whistleblowers may make an External Report to the Ombudsman or public authorities and, where appropriate, to institutions, bodies, offices or agencies of the European Union without first submitting the Report in accordance with this Appendix. However, the use of internal reporting channels established under this Appendix as set out above before reporting externally is strongly encouraged as it may expedite proceedings in response to the Report and allow conducting Follow-up Actions more efficiently and quickly.

An External Report may be submitted to the Ombudsman who will conduct initial review thereof and, in accordance with its authority, will either proceed with follow-up actions internally or will forward the External Report to the local or EU authority which is competent for taking follow-up actions in relation to a given External Report, of which the Whistleblower will be notified.

Detailed information on external reporting procedure is available on the website of the Ombudsman's Office: [Biuletyn Informacji Publicznej RPO | Rzecznik Praw Obywatelskich \(brpo.gov.pl\)](https://biuletyn.informacji.publicznej.rpo.gov.pl) and additionally on the websites of the Public Information Bulletin dedicated to a given public authority.

The provisions of this chapter enter into force on 25 December 2024 (as per the article 64 of the Whistleblowing Act).

14. Protections

14.1 Personal data protection and confidentiality

The whole Speak Up Line process and handling of Reports is subject to personal data protection regulations and requirements applicable to sensitive data. Reports and related investigation materials shall be stored by the investigating corporate function team in a secure, restricted access folder and the data retained for no longer than is necessary, proportionate and in accordance with applicable jurisdictional data retention timeframes. Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted within the applicable jurisdictional data retention timeframes.

The data shall be processed in a secure and restricted manner that ensures that the confidentiality of the identity of the Whistleblower and any third party mentioned in a Report is protected, and prevents access thereto by nonauthorised staff members. The Branch shall prevent unauthorized persons from gaining access to the information covered by the Reports and ensure protection of the confidentiality of the identity of the Whistleblowers, the persons concerned by the Reports and the third parties indicated in the Reports. The protection of confidentiality applies to all personal data based on which these persons' identity can be directly or indirectly revealed.

14.2 Prohibition of retaliation

Retaliation against a Whistleblower, including threats of retaliation and attempts of retaliation, whatever the nature, are strictly prohibited. No Retaliatory Action or attempted or threatened Retaliatory Action may be taken against the Whistleblower; provided that he/she reports matters in good faith, i.e., having reasonable grounds to believe that the reported Information on a Breach of Law is true at the time of submitting the Report and that it constitutes Information on a Breach of Law which is subject to this Appendix.

Annex

DEFINITIONS AND INTERPRETATION

Terms used in this Appendix shall have the following meaning:

Breach of Law	means an act or omission that is unlawful or intended to circumvent the law, relating at least to one of the areas defined in the Act which, as of the date of this Appendix are: corruption, public procurement, financial services, products and markets, prevention of money laundering and terrorist financing, product safety and compliance, transport safety, protection of the environment, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, protection of privacy and personal data, security of network and information systems, financial interests of State Treasury of the Republic of Poland, local government unit and European Union, the internal market of the European Union, including public law competition and state aid rules, and legal entities taxation, constitutional human and civil rights and freedoms in relations between an entity and authorities and unrelated to the above areas (Art. 3 Sec. 1 of the Act);
External Report	means oral or written notification containing Information on a Breach of Law to the Ombudsman or public authorities (Art. 2 Item 17 of the Act);
Feedback	means an information provided to the Whistleblower on the Follow-up Actions planned or taken and the reasons for such actions (Art. 2 Item 4 of the Act);
Follow-up Action	means any action taken by the Branch to assess the accuracy of the information contained in the Report and to prevent a reported Breach of Law, in particular through an investigation, initiation of inspections or administrative proceedings, prosecution, action taken to recover funds or the closing of proceedings under the Appendix (as defined Art. 2 Item 1 of the Act);
Information on a Breach of Law	means an information, including reasonable suspicion, about an actual or potential Breach of Law that has occurred or is likely to occur at the Branch, in which the Whistleblower has participated in a recruitment or other precontractual negotiation process, works or has worked, or with which the Whistleblower has or has had contact in the Work-related Context, or information concerning an attempt to conceal such a Breach of Law (Art. 2 Item 3 of the Act);

Report	means oral or written notification containing Information on a Breach of Law to the Branch via reporting channels as set out in the Appendix (Art. 2 Item 15 of the Act);
Retaliatory Action	means direct or indirect act or omission in the Work-related Context that is caused by the Report, External Report or public disclosure and that violates or may violate legal rights of the Whistleblower or causes or may cause unjustified damage to the Whistleblower, including unjustified initiation of proceedings against the Whistleblower (Art. 2 Item 2 of the Act);
Work-related Context	means past, present or future activities related to the performance of work on the basis of an employment relationship or other legal relationship constituting the basis for the provision of work or services or performing a function in or for the Branch or for the benefit of the Branch, or performing service in the Branch, under which the Information on a Breach of Law has been obtained and there is a possibility of experiencing Retaliatory Actions (Art. 3 Item 5 of the Act).

-----[end of document]-----