

WHISTLEBLOWER POLICY

The law of 28 November 2022 on the protection of persons reporting breaches of Union or national law established within a legal entity in the private sector is a transposition of the European Whistleblowing Directive 2019/1937.

The law provides protection to any person who has obtained information about a serious problem regarding possible irregularities or misconduct in a private company in a work-related context and wishes to report this information.

This whistleblower policy aims to provide transparency for employees (*) and third parties with regard to the existing channels for reporting such (alleged) irregularities at SBB without having to follow the normal company hierarchy.

(*) Employee means any SBB employee, other worker and hired independent service provider.

As such, SBB wishes to act against any unlawful, deceptive or other unauthorised practices or acts under the control of the company, ensure independent and confidential investigations and avoid conflicts of interest. However, this policy does not imply an obligation to report, but rather an opportunity for SBB employees and third parties to report irregularities within the company while guaranteeing certain safeguards.

For the purposes of this policy, the following **definitions** apply:

- **"information on breaches"** means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur, and about attempts to conceal such breaches;
- **"report"** or **"to report"** means the oral or written communication of information on breaches;
- **"internal reporting"** means the oral or written communication of information on breaches within a legal entity in the private sector;
- **"external reporting"** means the oral or written communication of information on breaches to the federal coordinator or the competent authorities;
- **"public disclosure"** or **"to publicly disclose"** means the making of information on breaches available in the public domain;
- **"reporting person"** or **"whistleblower"** means a person who reports or publicly discloses information on breaches;

- **"work-related context"** means current or past work activities in the private sector through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information;
- **"facilitator"** means a natural person who assists a reporting person in the reporting process and whose assistance must be confidential;
- **"person concerned"** means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated;
- **"retaliation"** means any direct or indirect act or omission which is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person;
- **"anonymous reporting"** means reporting for which nobody, not even the recipient, knows the identity of the author.

Personnel scope:

This policy applies to reporting persons who have received information on breaches in a work-related context. This means that the reporting channels and protection measures listed below apply to, among others:

1. Current employees of SBB;
2. Former employees in case information on breaches was obtained in the context of a working relationship that has been terminated in the meantime;
3. Candidate employees in case information on breaches was obtained during the recruitment procedure or other pre-contractual negotiations;
4. Self-employed people working at SBB (such as freelancers, consultants);
5. The shareholders and persons belonging to the administrative, management or supervisory body of SBB, including non-executive members, volunteers and paid or unpaid trainees;
6. Anyone working under the supervision and direction of contractors, subcontractors and suppliers;
7. Facilitators;
8. Third parties who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons;

Material scope:

The reporting channels can be used to report the following breaches:

1° breaches that concern the following areas:

- a) public procurement;
- b) financial services, products and markets, and prevention of money laundering and terrorist financing;
- c) product safety and compliance;
- d) transport safety;
- e) protection of the environment;
- f) radiation protection and nuclear safety;
- g) food and feed safety, animal health and welfare;
- h) public health;
- i) consumer protection;
- j) protection of privacy and personal data, and security of network and information systems;
- k) combating tax fraud;
- l) combating social fraud.

2° breaches affecting the financial interests of the Union as referred to in Article 325 of the Treaty on the Functioning of the European Union and as further specified in relevant Union measures and, where applicable, national implementing provisions;

3° breaches relating to the internal market, as referred to in Article 26 (2) of the Treaty on the Functioning of the European Union, including breaches of Union competition and State aid rules.

However, the following are **not** covered by this whistleblower policy:

- Complaints related to violence, bullying and sexual harassment, which an employee who believes he or she is a victim of such acts may submit to the person of trust designated for this purpose in the labour regulations or to the psychosocial prevention advisor of the external service for prevention and protection at work.
- Reports related to classified information;
- Reports based on information covered by medical confidentiality;
- Reports based on information covered by the secrecy of judicial deliberations.
- Complaints related to SBB services (e.g. complaints about invoices)

Internal reporting procedure

INTERNAL REPORTING

1. An employee/third party who believes there is an irregularity may file a report:

- a. Option 1: with the complaints handler appointed for this purpose by the company.

The complaints handler designated for SBB is:

- For complaints regarding the prevention of money laundering and terrorist financing:
Jan Depoorter: jan.depoorter@sbb.be (016/24.64.51)
- For all other complaints: Sofia Van Gerven: sofia.van.gerven@sbb.be (016/24.64.55)

A report must preferably be made by e-mail or in writing, but may also be made verbally by telephone or other voice messaging systems and, at the request of the reporting person, by means of a physical meeting within a reasonable period.

- b. Option 2: Via the IntegrityLog web tool: <https://sbb.integrity.complylog.com/> via the "submit case" button

The complaints handler designated for SBB is:

- For complaints regarding the prevention of money laundering and terrorist financing: Jan Depoorter: jan.depoorter@sbb.be (016/24.64.51)
- For all other complaints: Sofia Van Gerven: sofia.van.gerven@sbb.be (016/24.64.55)

The employee/third party filing a report through the internal reporting channel may also do so anonymously.

2. The complaints handler who receives a report will send an acknowledgement of receipt of the report to the reporting person within 7 working days of receipt.
3. The complaints handler registers the report with the date it was received and is the only person who knows the identity of the reporting person. The confidentiality of the identity of the reporting person and of any third parties named in the report shall always be safeguarded¹. Non-authorised personnel do not have access to the internal reporting channel. If the initial report contains ambiguities, the complaints handler shall seek clarification.
4. The complaints handler is responsible for following up each report diligently. He assesses the accuracy of the allegations made in the report and, where relevant, addresses the reported breach, e.g. through actions such as an internal enquiry, an investigation or the closure of the procedure.
5. As soon as possible, and no later than 3 months after the acknowledgement of receipt of the report or, if no acknowledgement of receipt was sent to the reporting person, three months from the expiry of the seven-day period after the report was made, the complaints handler shall provide the reporting person with the information regarding the follow-up actions planned or taken and regarding the reasons for such follow-up.

Procedure of investigation and decision

1. After receiving the report, the complaints handler starts an investigation into the alleged irregularities.

The complaints handler is authorised in this capacity to conduct an independent investigation in the company.

The complaints handler shall hear the person or persons who are reported to be involved in the reported irregularities.

The complaints handler shall obtain information and consult sources necessary in the context of this investigation. In this way, the complaints handler tries to verify the alleged irregularities flagged by the reporting person.
2. When informing and reporting, the complaints handler shall neither disclose the identity of the reporting person nor the identity of the accused person or persons.

¹ i.e. The identity is known only by the complaints handler

3. The complaints handler shall report his findings in writing to the executive committee (or in its absence, another governing body). Only if the report concerns a member of the executive committee (or the governing body) shall the report be addressed to the chairman of the aforementioned body.
4. The executive committee (or other governing body) of SBB shall make a decision and if necessary, take action based on the complaint handler's report.
5. The reporting person and the accused person or persons shall be informed of the conclusion of the investigation.

Protection

1. The reporting and the handling of a report is done with respect for secrecy and confidentiality.
2. The anonymity of the reporting person is guaranteed and his or her identity is known only by the complaints handler.

Only the reporting person can release the complaints handler, in writing only, from his/her obligation of confidentiality and from preserving the reporting person's anonymity.

3. SBB's management declares that a report made by an employee to the complaints handler under the present whistleblower scheme shall not negatively affect the performance or career opportunities of that employee within the company.
4. The reporting person is requested to keep his report confidential and not to disclose it either directly or through third parties until SBB's executive committee has communicated the completion of the investigation.
5. A reporting person who has deliberately made a manifestly unfounded report and has consequently used the reporting procedure of the present whistleblower scheme unlawfully, may be sanctioned for this (see below).

Record keeping of reports

SBB shall keep records of every report received, in compliance with the said confidentiality requirements. Reports are kept for the duration of the contractual relationship.

Where an unrecorded telephone line or another unrecorded voice messaging system is used for reporting, the company reserves the right to document the oral reporting in the form of accurate minutes of the conversation, prepared by the staff member responsible for handling the report. The reporting person always has the opportunity to check, rectify and agree the minutes of the conversation by signing them.

Where a person requests a meeting with the complaints handler to file an internal report, SBB shall ensure, subject to the reporting person's consent, that complete and accurate records of the meeting are kept in a durable and retrievable form. SBB reserves the right to document the oral report in the following manner:

- by making a recording of the conversation in a durable and retrievable form; or
- through accurate minutes of the meeting prepared by the staff member responsible for handling the report. The reporting person always has the opportunity to check, rectify and agree the minutes of the meeting by signing them.

Right to the protection of privacy

The personal data of the reporting person and of the accused person or persons shall be processed confidentially and solely for the purpose of handling a report and the subsequent investigation in accordance with the Privacy Notice. These persons concerned may each invoke the right to access and correct processed data relating to their person in accordance with the General Data Protection Regulation 2016/679 and the Privacy Notice. They can also contact the Data Protection Authority for this purpose. They do not have access to third-party data.

PRIVACY NOTICE

SBB² will process personal data of (1) the person reporting the complaint (if not anonymous) and (2) the person concerned (i.e. the accused person) in its capacity as data controller. Specifically, SBB will process the following personal data associated with the reporting person's (anonymous) complaint:

- the surname/first name/e-mail of the reporting person (if the complaint is not submitted anonymously); and
- the content of the complaint; and
- the (personal) data related to the complaint (including the accused person and evidence).

SBB does not process special categories³ of the reporting person's personal data. If special categories of personal data are collected by SBB under the "Whistleblower Policy", such personal data will be processed with the necessary security and in accordance with the appropriate legal basis.

SBB always processes the above personal data in accordance with applicable European and national privacy legislation including but not limited to (1) the General Data Protection Regulation (EU) 2016/679 (hereinafter "**GDPR**") and (2) the law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.

A complaint can be filed anonymously by the reporting person. SBB always guarantees that the reporting person's information will not be made public. If possible, limited feedback will be provided by SBB regarding the action taken by SBB following the submitted complaint.

² Shall include (1) SBB Bedrijfsdiensten BV (*SBB Corporate Services – private limited liability company under Belgian law*) with registered office located at Diestsevest 32 box 1A, 3000 Leuven, with company number 0420.170.841 and (2) SBB Gecertificeerde Accountants en Adviseurs BV (*SBB Certified Accountants and Advisors – private limited liability company under Belgian law*) with registered office located at Diestsevest 32 box 1A, 3000 Leuven, with company number 0459.609.556 (herein referred to collectively as "SBB")

³ Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data, data on health or data on sexual behaviour or sexual orientation.

In addition, SBB processes the aforementioned personal data in a confidential manner and solely for the purpose of implementing the "Whistleblower Policy" resulting from compliance with legal obligations under (1) the Whistleblowing Directive 2019/1937 on the protection of persons reporting breaches of Union law and (2) the Law of 28 November 2022 on the protection of persons reporting breaches of Union or national law established within a legal entity in the private sector.

Specifically, SBB processes these personal data to fulfil the purposes arising from the aforementioned legislation and its "Whistleblower Policy" and to be able to process, assess and, where necessary, further investigate the reporting person's (anonymous) complaint (i.e. personal data are processed under Article 6.1 (c) GDPR "necessary for compliance with a legal obligation").

In practice, SBB will receive the personal data mentioned herein through its processor, Euronext Corporate Services Sweden AB (ID 559141-7083), which supplies the IntegrityLog software, for the purpose of processing and assessing the reporting person's (anonymous) complaint. SBB and its processor, Euronext Corporate Services Sweden AB, have implemented appropriate technical and organisational measures to protect the personal data received and to safeguard the purposes of the "Whistleblower Policy". Specifically, SBB has implemented security standards that ensure personal data is protected against loss, misuse, alteration and unauthorised access.

Personal data will only be processed in the European Economic Area and kept for as long as necessary to process the reporting person's (anonymous) complaint. SBB undertakes to delete the personal data from its systems within two months of the completion of the (anonymous) complaint and investigation. This retention period may be extended if justified or required by law to respect a longer retention period.

Under certain conditions, the reporting person has the right to (i) access his/her personal data; (ii) correct his/her personal data; (iii) delete his/her personal data; (iv) restrict the processing of his/her personal data; (v) object to the processing of his/her personal data; (vi) exercise the right to portability of his/her personal data; (vii) request the transfer of his/her personal data and (viii) withdraw his/her consent (if applicable) at any time.

The reporting person may exercise the above rights by contacting privacy@sbb.be and providing the necessary supporting documents to SBB. Please note that as a result of the exercise of certain of the above rights, SBB will not be able to respect its obligations under the "Whistleblower Policy" and/or applicable legislation and in this case SBB will notify the reporting person that the exercise of the above rights is not possible in view of the current applicable regulations. SBB will make all reasonable and practical efforts to fulfil the request provided that it complies with applicable law and professional standards.

Furthermore, the reporting person may also file a complaint with SBB or the Belgian Data Protection Authority if he/she believes that the processing of his/her personal data violates the GDPR (<https://www.gegevensbeschermingsautoriteit.be/contact>) / <https://www.autoriteprotectiondonnees.be/contact>). Subsequently, the reporting person always has the option of contacting SBB's data protection officer at privacy@sbb.be.

More information about what the rights specified above entail and how SBB processes personal data is available at <https://www.sbb.be/en/privacy-statement>. SBB may amend this notice from time to time to clarify its current privacy practices, and the reporting person will be notified in due course of such changes.

External reporting procedure

An employee/third party may also report information on breaches by using the external reporting channels and procedures after they have first filed a report through internal reporting channels, or by immediately making a report through external reporting channels.

COMPETENT AUTHORITIES

The authorities competent for receiving reports, giving feedback and providing follow-up regarding reports are [the following](#).

PROCEDURES FOR EXTERNAL REPORTING TO THE FEDERAL COORDINATOR AND COMPETENT AUTHORITIES

An employee/third party who believes that an irregularity has occurred may file a report with the competent authority or the Federal Ombudsman according to the following [procedure](#).

The competent authorities publish on a separate, easily identifiable and accessible page of their website at least the following [information](#).

Public disclosure

In addition to the possibility of filing a report through the internal reporting channel or the external reporting channels, every person has the option of publicly disclosing the information related to a breach.

A reporting person making a public disclosure is eligible for the following protection under this policy, if:

- 1° the employee first filed an internal and external report, or immediately filed an external report, but no appropriate action was taken in response to that report within the specified time frame;
- or

2° the employee has valid reasons to believe that: (a) the breach may pose an imminent or real danger to the public interest; or (b) in the case of external reporting, there is a risk of retaliation, or it is unlikely that the breach will be effectively remedied, due to the particular circumstances of the case, because, for example, evidence may be withheld or destroyed, or an authority may collude with the perpetrator of the breach or be involved in the breach.

Conditions

If a reporting person:

- had a valid reason to believe that the reported information on breaches was accurate at the time of reporting and that said information was within the scope of this policy⁴; and
- reported information internally or externally in accordance with this policy, or disclosed information accordingly;

he or she also enjoys specific protection against retaliation measures.

The reporting person does not lose the benefit of protection on the sole ground that the report made in good faith was found to be incorrect or unfounded.

Facilitators and third parties associated with the reporting persons are also eligible for the protections set out below if they had reasonable grounds to believe that the reporting person fell within the scope for protection of this policy.

Protective measures against retaliation

If the reporting person, facilitator or third party associated with the reporting person meet the above conditions, they enjoy protection against any form of retaliation, including threats and attempts of retaliation. Retaliation includes the following [measures](#).

⁴ This first criterion is assessed with a person who is in a similar situation and has similar knowledge

No civil, criminal or disciplinary claims or professional sanctions may be brought against persons who report information on breaches or make a public disclosure in accordance with this policy because of such reporting or public disclosure.

Reporting persons cannot be held liable for the acquisition of or access to the information reported or publicly disclosed unless such acquisition or access constituted a criminal offence in itself.

Any protected person who believes he or she has been victimised or threatened with retaliation may file a duly justified complaint with the federal coordinator, who will initiate an extrajudicial protection procedure in accordance with Article 26 et seq. of the law of 28 November 2022 on the protection of persons reporting breaches of Union or national law established within a legal entity in the private sector.

Without prejudice to any other administrative or extrajudicial remedy, any protected person has the right to file an appeal before the labour court in case of retaliation in accordance with Article 578 of the Judicial Code.

Support measures

All protected persons have access to the following [support measures](#).