Whistleblowing policy SBE s.a.

Rev.0.2: 15-09-2023

Legal framework:

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.
- Act of 28 November 2022 on the protection of reporters of breaches of Union or national law established within a legal entity in the private sector.
  This law will enter into force on 15 February 2023, two months after publication in the Belgian Official Gazette on 15 December 2022.
  Regarding the provision of internal reporting channels, a derogation is provided for legal entities in the private sector with 50 to 249 employees: those specific rules will only apply to them from 17 December 2023.

Objective of this Whistleblower Policy:

Integrity, ethical conduct, are among the cornerstones of SBE's operation. Partly for this reason, SBE has established an internal whistleblowing system that allows both employees and external parties to report breaches of internal policies and procedures, as well as applicable laws and regulations, in a confidential and effective manner in which the reporter is protected from retaliation. How, when and by whom a report can be made and how it is handled is included in this policy.

The open-door policy within SBE gives colleagues the opportunity to discuss misconduct directly with a manager, confidant or contact person within the HR department.
In addition, within the framework of, and in accordance with the applicable legislation, a reporting policy has been established within SBE nv. The details of this are set out further in this policy document.

Who can file a report?

All stakeholders who have a professional relationship with SBE SA. It concerns a cooperation already started or terminated. This policy also applies to prospective employees, in case information on infringements has been obtained during the recruitment procedure.

In summary, reports can be made by:

- all employees of SBE S.A.
- former employees of SBE S.A., if they have obtained information about infringements during or after their working relationship with SBE S.A.
- partners

- subcontractors
- freelancers, working for SBE S.A.
- trainees
- applicants, if they have obtained information about infringements during the recruitment procedure

What can be reported ?

The following topics fall within the scope of the Whistleblower Policy:

- internal fraud (e.g. theft, falsification of information, falsification of payments, deliberate harm to SBE S.A.)
- infringements relating to the legal scope:
    - public procurement
    - financial services, products and markets, prevention of money laundering and terrorist financing
    - product safety and product conformity
    - transport safety
    - protection of the enviroment
    - radiation protection and nuclear safety
    - food and feed safety, animal health and welfareVolksgezondheid
    - public health
    - consumer protection
    - protection of privacy and personal data, security of network and information systems
    - combating taks fraud
    - combatting social fraude
- infringements affecting the interests of the European Union
- breaches relating to the internal market (of the European Union), including breaches of Union rules on competition and state aid
- breach of the code of conduct and other procedures and policies of SBE S.A.
- a breach of SBE S.A.'s contractual obligations

Exceptions:

The law relating to Whistleblowing does not apply to:

- the field of national security (except public procurement in the field of defence and security)
- information covered by medical professional secrecy
- information covered by the professional secrecy of lawyers

Protective measures in respect of the Whistleblower:

SBE SA aims to create an environment in which the Whistleblower feels safe to report a Misconduct (see list "what can be reported") within the organisation. To this end, the following protective measures have been taken:

- the confidential treatment of the identity of the Whistleblower:
  - reports are managed by the Notification Manager (description and tasks see below in this document); the files are kept in the dedicated Whistleblower tool (see below in this document), which can only be accessed by the Notification Manager and his/her appointed investigation team;
  - all internal and external parties involved in the investigation and follow-up responses (= the above-mentioned investigation team) are subject to strict confidentiality obligations (see annex 1 of this document);
  - the identity of the Whistleblower will not be disclosed unless:
    - the Whistleblower expressly consents to this; or
    - the disclosure is required by law

- the possibility for the Whistleblower to remain anonymous when filing a report, as well as during further investigations. In this case, the Whistleblower Tool guarantees that the identity of the Whistleblower remains protected and cannot be found out by anyone involved in the investigation. Therefore :
  - at no time will the Whistleblower be specifically asked to reveal his/her identity
  - the Whistleblower Tool guarantees that the identity of the Whistleblower is protected and cannot be traced in any way
  - during the follow-up procedure, the Whistleblower may refuse to answer questions which, in his/her opinion, may identify him/her

  SBE SA will make all reasonable efforts to investigate an anonymous report, but notes that in some cases there are limits to what can be achieved when the Whistleblower chooses to remain anonymous.

  No whistleblower, third parties related to the whistleblower (family of, colleague, friends,...), or anyone who helped the whistleblower to file a report as defined in the legal scope, can be penalised or be the subject of any discriminatory measure.
  SBE SA does not permit any retaliation against those who, in good faith, report a breach or suspected breach of the rules or guidelines.

- if a Whistleblower, third parties associated with the Whistleblower or anyone who has assisted the Whistleblower fear retaliation or believe that retaliation has already been taken against them, they should

immediately report their concerns to the Reporting Manager. The latter will then investigate this neutrally and ensure that appropriate action is taken to prevent or remedy retaliation.

Immunity from liability in case of reporting or disclosure in accordance with the terms of the Act. This means, among other things, that if, after investigation, it appears that the reported infringement is not proven or considered to exist, the Whistleblower, if in good faith, cannot be held liable for any image or other damage resulting from the report.
Reporters who have knowingly reported false information may be punished under prevailing criminal law (defamation and libel), and lose protection in case of public reporting, disclosure in bad faith.

Reporting channels:

- internal reporting channels
- external reporting channels
- disclosure

Internal reporting channels:

- **verbally**: an accurate and as complete as possible transcript is made of oral reports by the Notification Manager, submitted for review, correction and signature to the Notification Manager. The latter enters the signed transcript, in the Whistleblower tool
  - by phone: via Microsip 7796 (Notification Manager)
  - physical meeting: by appointment via:
    - Whistleblowing@sbe.be
    - Microsip 7796 (Notification Manager)
- **in writing:**
  - via Whistleblowertool (ticketingsystem Jira, "Submit anonymous whistleblowing report")
  - via mail: Whistleblowing@sbe.be
    the Notification Manager enters this mail in the Whistleblower tool. In this way, like normal reporting via the ticketing system Jira, a unique report ID is created

External reporting channels:

It is strongly recommended to report misconduct/breaches first via the Whistleblower tool within SBE S.A. (see internal reporting channels). Internal reporting remains the most efficient to allow SBE S.A. to thoroughly investigate the matter and take appropriate action to address the misconduct/infringement.

Within the European Union, a whistleblower has the option of reporting misconduct falling within the scope of Directive (EU) 2019/1937 to a local competent authority responsible for receiving and investigating Whistleblower reports.

List of local competent authorities for external reporting	
Belgium	With the Royal Decree of 22 January 2023, the government has designated the bodies that act as competent authorities for external reports on breaches within the framework of the Whistleblowing Regulations for the private sector. These are the following authorities, each competent for its own domain : • FPS Economy, SMEs, Self-employed and Energy • FPS Finance • FPS Health, Food Chain Safety and Environment • FPS Mobility and Transport • FPS Social Integration, Poverty Reduction, Social Economy and Metropolitan Policy Programme • Federal Agency for Nuclear Control • the Federal Agency for Medicines and Health Products • the Federal Agency for the Safety of the Food Chain • the Belgian Competition Authority • the Data Protection Authority • the Financial Services and Markets Authority • the National Bank of Belgium • the College of Auditors' Supervision • the authorities reported in article 85 of the law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash • the National Committee for Security of Drinking Water Supply and Distribution • the Belgian Institute for Postal Services and Telecommunications • the State Institute for Sickness and Disability Insurance • the State Institute for Social Security for the Self-Employed • the National Office for Employment • the National Agency for Social Security • the Social Intelligence and Investigation Service

	• the Anti-Fraud Coordination Agency (FCA) • the Shipping Inspectorate the Federal Ombudsman assumes a coordinating role. it is his task to : • receive external reports of integrity violations • check whether they are admissible and whether there is a reasonable suspicion that the reported violations have occurred • and, if the latter, forward them to the body competent to investigate the report • In exceptional cases, such as when no authority has jurisdiction, the Federal Ombudsman will act as the competent authority and also investigate the report integriteit@federaalombudsman.be
Netherlands	• House for Whistleblowers www.huisvoorklokkenluiders.nl • Consumer and Market Authority (CMA for breaches of consumer law : www.acm.nl • Personal Data Authority (AP) for breaches of personal data protection www.autoriteitpersoonsgegevens.nl • "De Nederlandsche Bank N.V." (DNB) and Authority for Financial Markets (AFM) for violations of economic and financial law regulations www.dnb.nl www.afm.nl • Healthcare and Youth Inspectorate www.igj.nl • The Dutch Healthcare Authority www.nza.nl • The Nuclear Safety and Radiation Protection Authority www.autoriteitnvs.nl
Spain	• La Autoridad Independiente de Protección del Informante, AAI canaldedenuncias@airef.es

Disclosure:

A disclosure is making information about abuses publicly available (e.g. via press or social media).

Reporting breaches through a disclosure will only lead to the protection of the reporter in specific circumstances.

A reporter may disclose breaches after initially making an internal and external report, or an external report immediately, if no appropriate action has been taken on the report within the prescribed period (three months in the case of an internal report)

A person may proceed directly to a disclosure as described above if he or she has reasonable grounds to believe that:

- the breach may pose an imminent or real danger to the public interest; or
- there is a risk of retaliation in the case of external reporting, or the breach is unlikely to be effectively remedied, due to the particular circumstances of the case (destruction or withholding of evidence, risk of the authority colluding with the perpetrator of the breach or being involved in the breach.

The internal reporting channel:

The Notification Manager:

Profile and duties:

- impartial person, with no conflict of interest. He/she should not receive instructions on the handling of a concrete case and should be able to report directly to the highest management level on (potential) risks or obstacles to his/her tasks.
- responsible for careful follow-up of the report
- maintains communication with the reporter
- requests other information if necessary and provides necessary feedback

Within SBE S.A. Inge Palmans has been appointed as notification manager and can be reached at :

- by phone: +32 3 777 95 19 by connecting to Microsip n°7796
- E-mail: Whistleblowing@sbe.be

The whistleblower Tool:

Where to find this tool:

- SBE's Jira service desk platform
  https://sbe-engineering.atlassian.net/servicedesk/customer/portals
  or
- website SBE, policies
  https://www.sbe-engineering.com/

tool name: "Submit anonymous whistleblowing report" (*)

(*): for instructions for use, see Annex 2 of this document

Recommended content of a report:

- name + first name of the reporter (*)
- role or involvement in the incident mentioned in the report
- a detailed description of the incident or violation the Whistleblower wishes to report, together with the time, date and location of any specific incidents or violations.
- the name and contact details of other persons who witnessed, or who have more information , about the incident.
- any information the reporter might have about similar previous incidents or breaches relating to the person(s) mentioned in this report.
- any documentary evidence or useful documents available to the reporter in connection with the report.

(*) if the reporter chooses to remain completely anonymous, the ticket number serves as the only link to the anonymous reporter. It is therefore important for the reporter to write down or remember the ticket number properly in order to communicate with the Notification Manager, and receive feedback regarding the report.
Given the practical difficulties of an anonymous report and the way in which the processing of personal data is handled within SBE S.A.'s Whistleblower Policy (for further explanation, see further in this policy statement), anonymous reports are discouraged (despite permitted).

The internal follow-up process:

Acknowledgement of receipt:

Upon receipt of a report, the Notification Manager will initially check whether the report falls within the scope of this Whistleblower Policy. If it does not, the Notification Manager will inform the notifier accordingly:

- if the report was made via the whistleblowing tool ("submit anominous whistleblowing report"), the unique ID generated by the tool counts as the acknowledgement of receipt.
- in the case of a verbal report or report via e-mail (whistleblowing@sbe.be), the Notification Manager sends, within seven days of receiving the report, a confirmation of receipt via e-mail to the Whistleblower, including the file number.

Research:

Upon acceptance of the report, it will be promptly and carefully investigated. All investigations will be thoroughly investigated in accordance with the principles of confidentiality, impartiality and fairness to all persons involved. If deemed necessary, the Notification Manager may appoint an investigator or investigation team who has relevant experience in conducting such investigations, or has specialist knowledge of the subject matter. The members of the investigation team should sign a confidentiality statement (*) upon appointment so as not to compromise the serenity and confidentiality of the investigation.
(*) see annex 1 of this document

Feedback:

If the report was made via the Whistleblower tool, the Whistleblower can always check the report status via the unique report ID generated when the report was created.
In case of a verbal report or report via e-mail (whistleblowing@sbe.be), the Whistleblower will receive feedback on the (ongoing or completed) investigation of his/her report no later than three months after the confirmation of receipt. The Whistleblower has the right to be kept informed of the status of the investigation. However, the Whistleblower is not entitled to be informed of the integral content of the investigation, in order not to harm the progress of the investigation.

Decision:

Upon completion of the investigation, the Notification Manager/Investigation Team, makes a final decision on whether the misconduct has been proven and what relevant actions are required to end the misconduct and protect the company.
The Notification Manager will prepare a final report describing the facts and the final decision:

- in case the misconduct is proven, relevant actions are identified with a view to ending the misconduct and protecting the company,
- in case the investigation shows that there is insufficient or no evidence of the misconduct, no further action is taken.

The Whistleblower will be informed of the decision taken via the Whistleblower Tool.

File storage:

Files of the reports submitted by Whistleblowers are kept only in the Whistleblower Tool, so that the reports are kept strictly confidential.
All data will be kept no longer than necessary and proportionate and will be deleted two years after the conclusion of the investigation.

The investigation is considered closed when:

- has been decided not to take any further action,

  or

- all action points reflected in the final decision have been implemented or completed.

Notice on data protection in the context of Whistleblowing:

This section is designed to inform you of, and comply with, our legal obligations in relation to data protection and Whistleblowing.
If you are a whistleblower, a reported person, or other named third party, we process personal data about you. this data protection section explains how your personal data is processed under this policy.

As the data controller, SBE SA (hereinafter referred to as "we") is responsible for the processing of personal data that we request and use for Whistleblowing purposes.

In any case, we take the measures to ensure that you:

- stay informed of our processing of your personal data and of your rights;

- continue to control the personal data we process;
- can exercise your rights in relation to your personal data. More information on your rights can be found further in this document.

What data do we collect about you?

Personal data:

By "personal data" we mean any information relating to an identified natural person ("the data subject"). An identifiable person is a natural person who can be directly or indirectly identified, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one of more elements characterising the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person. When we receive a report from you, a file containing the details of your report is created. This file will contain your identity, contact details and any other information you have given us about the person(s) involved in the report. We will keep the information provided confidential.

You can contact us anonymously via the Whistleblower Channel if you wish, we guarantee confidentiality and anonymity, in case the reporter wishes to remain anonymous.

We treat the information you provide confidentially and will not disclose it without lawful grounds. In case of further investigation and contact with other persons inside or outside the organisation, certain elements related to the report may need to be communicated. If certain information in the report should not be disclosed in the context of an investigation, we ask you to indicate this explicitly in the report.

Sensitive data:

As a data controller, we do not intend to collect and process so-called sensitive data, such as:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- processing of genetic data, biometric data for the purpose of uniquely identifying a person;
- data relating to health;
- data relating to a person's sexual behaviour or sexual orientation.

However, should we receive such data as part of a report, we will treat such sensitive data with the highest degree of security and confidentiality.

Why do we need your data?

We need sufficient information from you to investigate your report to us, including any evidence you have to support it.

We need to know the details of your report so that we can investigate it in depth and make a decision on the organisation's compliance with the relevant laws and we can fulfil our obligations.

What is the legal basis for processing your personal data?

Personal data mentioned in Whistleblower notifications on subjects related to an incident are processed on the basis of legal obligation, as this information is necessary to comply with the Belgian legislation of 28 November 2022, on the protection of reporters of breaches of Union or national law established within a legal entity in the private sector, i.e. assessing Whistleblower notifications and carrying out any investigations.

By accessing and using the Whistleblower Channel in an identified manner, the reporter consents to the processing of his/her personal data for the purposes indicated in this Whistleblower Policy.

With whom we share your personal data?

Initially, only the Notification Manager (Inge Palmans) appointed by SBE SA has access to the personal data mentioned in the notification. These data may be shared with, if relevant, the members of the investigation team in the context of an investigation. The latter will have to sign a confidentiality declaration (annex 1 of this document) before their appointment by the Notification Manager.

Only where we are required to do so by law, your personal data may be disclosed to supervisory authorities, tax authorities and investigation services if it is a necessary and proportionate obligation under special legislation in the context of investigations by national authorities or judicial proceedings, also to safeguard the rights of defence of the data subject(s).

Where your data is stored and processed?

Your data will not be stored and processed outside the European Union and we will in any case ensure that minimum legal requirements and security standards are met at all times.

Outside the cases mentioned above, your personal data will never be passed on or made available to third parties and will only be used for these purposes.

How long we keep your personal data?

Personal data obtained in the context of whistleblowing will be retained for as long as necessary to process the report, including any consequences thereof, and in line with the retention period of reports in the Whistleblower Tool (generally two years after the conclusion of the investigation).

How do we secure your personal data?

We have implemented generally accepted technological and operational security standards to protect personal data from loss, misuse, alteration or destruction without consent.

The Whistleblower Channel has been set up so that only the Notification Manager acts as data processor, or the persons specifically designated in accordance with Article 28 of the General Data Protection Regulation (GDPR), will ensure the full confidentiality of the personal data provided in accordance with the most appropriate security measures implemented for that purpose.

What are your rights?

Under the GDPR, data subjects have the following rights in relation to their personal data:

- right of inspection;
- right to rectification of inaccurate personal data;
- right to data erasure ("Right to oblivion").
  The right to data erasure will not be implemented in most cases, as the controller bases its processing on a legal basis;
- right to restriction of processing;
- right to data portability;
- right to object.
  The right to object will not be implemented in most cases, as the controller bases its processing on a legal basis. The controller guarantees to respond to the request within one month, after receiving the request. This in accordance with the obligations in Article 12 point 3 of the GDPR. Depending on the complexity of the enquiries and the number of requests, this deadline may be extended by a further two months if necessary. The controller shall notify the data subject of such an extension within one month of receiving the request.

How to exercise your rights?

When you exercise your right, please indicate this clearly in the notification. Please indicate which right you are invoking and to which processing(s) you object or wish to withdraw consent. Always be as specific as possible when you want to exercise your rights.

How to submit questions or complaints?

For questions or complaints about our processing of personal data, about the exercise of your rights or about this Declaration, we also refer you to our Whistleblower Platform and your personal ticket number. This way, we can ensure the confidentiality of communications.

We aim to find a fair solution to any report or concern about privacy. However, should you feel that we have not been able to help you, you have the right to file a report with the data protection authority.

Review:

This Whistleblower Policy will be reviewed at least once every three years. If necessary, these revisions will be coordinated and validated by SBE SA's in-house lawyer.

Users should always consult the latest version of this policy. In case of doubt whether the latest revision is being used, this can always be inquired with the Notification Manager via the contact details mentioned in this Whistleblower Policy.

Attachment 1 of document "Whistleblowing policy SBE s.a."

Confidentiality statement of a member of the investigation team appointed by the notification manager

Concerning: whistleblower file xxx *(to be filled in by notification manager)*

The signatories:

1. *(Name)* located at *(Street, house number, postcode and city)*, hereinafter referred to as "Investigator",

And

2. *(Name)* located at *(Street, house number, postcode and city)*, hereinafter referred to as "Notification Manager",

Declare that they have agreed as follows:

Article 1. Nature of provision of information
Investigator agrees to be provided with confidential information (hereinafter: the Information) by Notification Manager regarding: the whistleblower file xxx*(to be filled in by Notification Manager)*
The purpose of providing this information is: To support Notification Administrator in assessing Whistleblower's report in the above-mentioned file.

Article 2. Confidentiality
Investigator shall treat all information referred to in Article 1 that has been or will be provided to him by Reporting Manager or its designated persons as confidential information which he shall therefore keep strictly confidential from third parties.

Article 3. Research staff
Investigator shall disclose the Information only to Notification Manager or its designees for the realisation of the purpose described in Article 1. Investigative Staff will sign this confidentiality agreement before receiving the Information.

Article 4. Duration of the agreement
Investigator shall be bound to secrecy of the Information for the duration of 10 years from the signing of this agreement, or until the information provided has become of public knowledge through no fault or omission of Investigator. Investigator is not bound to secrecy on matters which he can prove were already in the public domain before the information was received by Notification Manager..

Article 5. Termination
Notification Manager is entitled at any time to decide not to provide further Information and to demand the information previously provided. Furthermore, Investigator shall return any use of the written information provided to him/her to Notification Manager immediately upon termination of the agreement.

Article 6. Penalty clause
If Investigator fails to comply or fully comply with the obligations in this agreement, an immediately payable claim of:

- Compensating all damages and costs resulting from the breach of this clause.
- An immediately payable fine of EUR 5,000, - per violation, to be increased by EUR 500, - for each day or part thereof that the violation may continue.

Article 7

- This agreement is governed by Belgian law
- All possible legal disputes arising from this agreement will be settled by the district court in *(Place)*.

Thus agreed and drawn up in duplicate at (Place) on (date)

Name Investigator
Signature Investigator

_____

Name Notification Manager
Signature Notification Manager

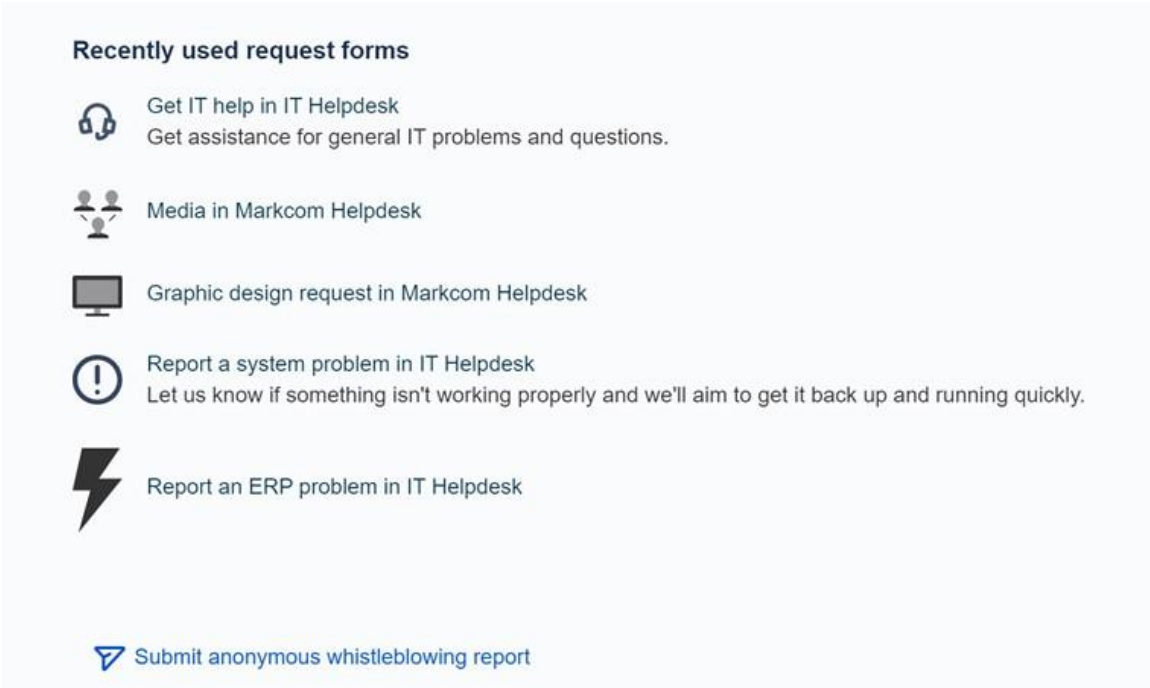
_____

Attachment 2 of document "Whistleblowing policy SBE s.a."

Whistleblowing guidelines:

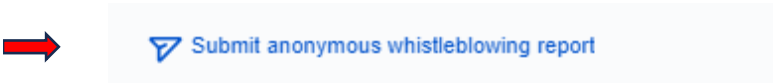
Log in to the SBE Jira service desk platform via support.sbe.be or on the website www.sbe-engineering.com:

1. Scroll down on SBE's Service/Support desk platform and select "Submit anonymous whistleblowing report"

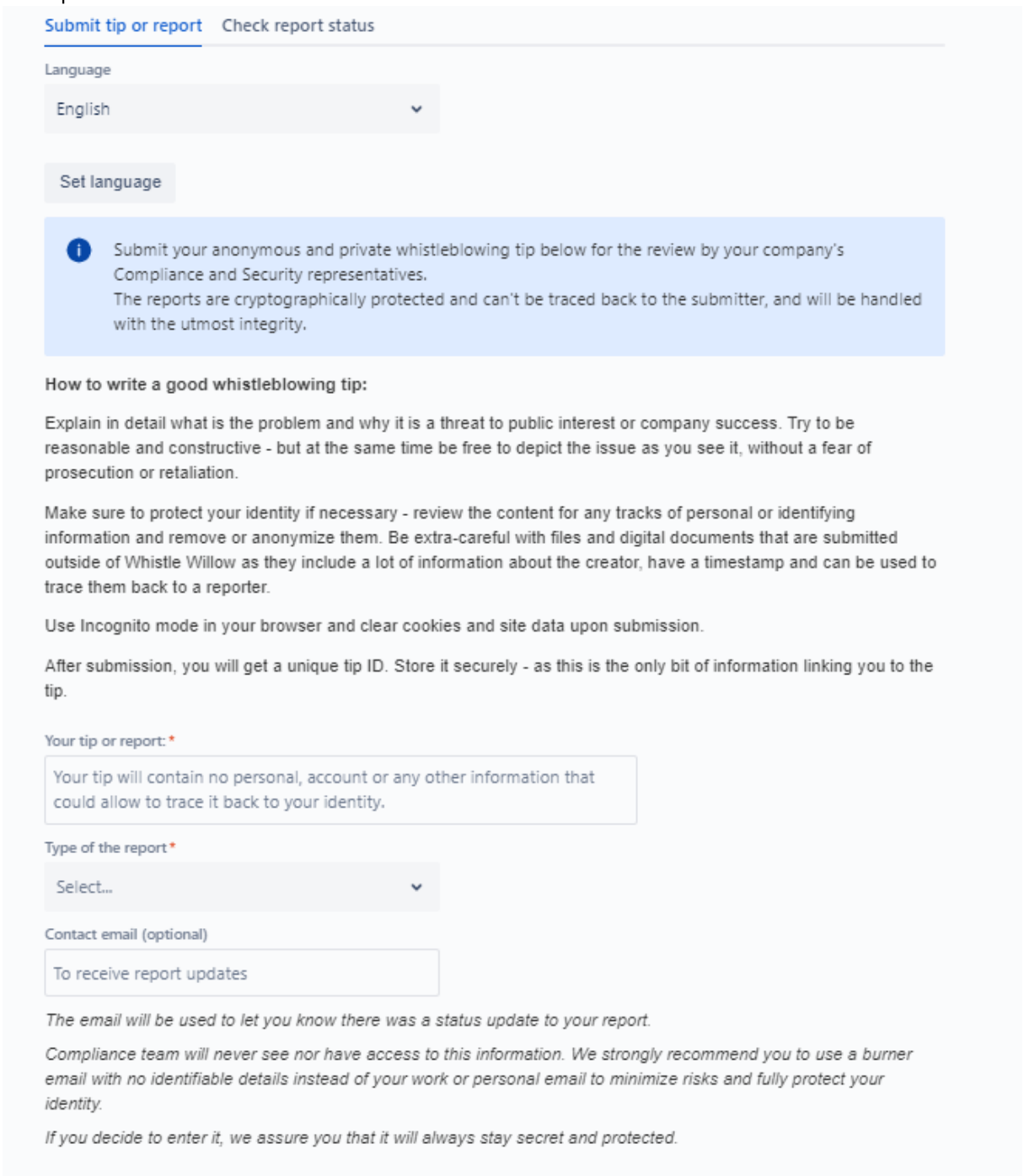


Or

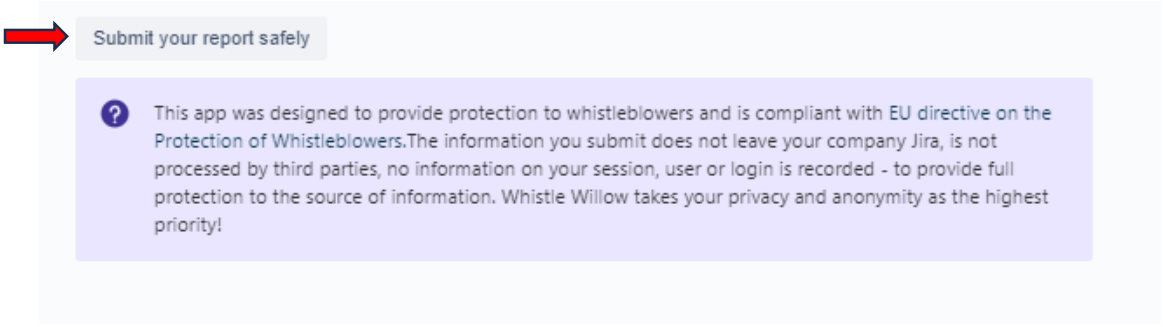
Go to the policies on SBE's website and select the Whistleblowing policy:



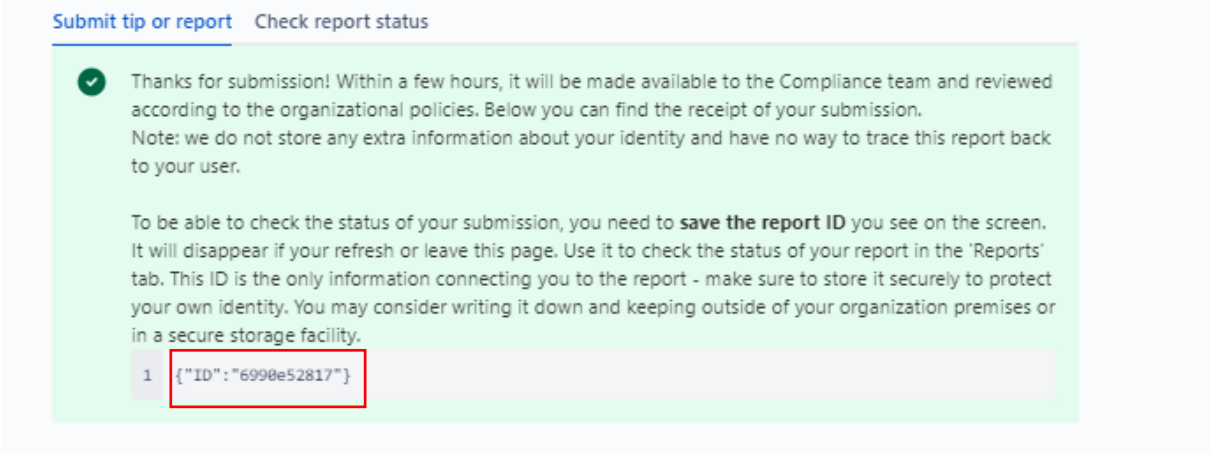
2. Complete the form:



3. Submit your report:



4. Confirmation:
   You will receive a unique ID, which you are requested to save.



5. Check report status: