WHISTLEBLOWING PROCEDURE

Date	Person responsible	Summary description of changes
16/12/2024	CEO	First Edition

INDEX

1. Context of reference

On 30 March 2023, Legislative Decree 24/2023 entered into force, implementing European Directive 2019/1937, and introduced the new "whistleblowing" regulation in Italy ("**Whistleblowing Law**").

This introduces a single regulation that consolidates the entire framework of rules that allow individuals to file reports of offences and irregularities ("**Reports**") and offer the protections to the these individuals. More specifically, the Whistleblowing Law sets out, among other things:

- the categories of natural persons – internal or external to the entities and companies – who have a legal relationship with them and who can file a report ("**Whistleblowers**");
- the protections given to Whistleblowers, reported persons and other parties involved and the obligations of the entities and companies in terms of prohibitions on retaliatory and discriminatory conduct and protection of their confidentiality;
- the types of conduct and information that form the subject of Reports, and the minimum requirements for Reports to be considered;
- the requirement to have one or more channels (in computerised form) that enables whistleblowers to file reports and guarantees the confidentiality of the identities whistleblowers and all persons involved and mentioned in the report, as well as the content of the report and all relevant documentation;
- the modalities that alleged violations can be reported through and the persons in charge of receiving Reports;
- the procedures for inquiries and possible investigations when a Report is filed;
- the need to consult representation and trade union organisations referred to in Art. 51 of Legislative Decree No. 81 of 2015 before activating the reporting channels;
- the conditions for external reporting; and
- the need to ensure that the disciplinary system adopted under Art. 6(2)(e) of Decree No. 231 of 2001 imposes penalties against those found to be responsible for the offences listed under Art. 21(1) of the Whistleblowing Law.

2. Objectives

This document sets out the operational procedures for: (i) managing Reports, and any ensuing inquiries and investigations, that come to their knowledge as a result of the functions performed, with a view to bringing to light any unlawfulness or irregularities within the Company; (ii) clarifying and facilitating the reporting by the reporting party; and (iii) removing any factors that could hinder or discourage recourse to the institution.

This procedure therefore: (i) provides the Reporting Officer with clear operational instructions on the subject, content, recipients and methods for filing Reports; and (ii) informs him/her of the forms of protection and confidentiality that are recognised and guaranteed to him/her and to all persons involved in the Reports.

The reporting system implemented by the Company and described in this document has the following features:

1. It remains accessible by anyone who wishes to file a Report.
2. It guarantees the highest levels of confidentiality regarding the information disclosed and the identities of the reporter and the person reported.
3. It offers Whistleblowers the choice between written or oral form by using a web platform that resides outside the Company's IT system and is hosted on an independent server.
4. It enables continuous interaction between the Company and the Whistleblowers.

5. It is managed by an autonomous, dedicated and specially trained person who manages the reporting channel ("**System Manager**"), identified in the Company's Supervisory Body. During the reporting management process, the System Administrator is assisted by the Reporting Committee – comprising the Supervisory Board, CTO and Corporate Development Manager – and by the corporate functions involved from time to time.
6. It complies with the requirements of the Whistleblowing Act.

The content of this document is shared with all employees and third parties that have a legal relationship with the Company through a publication on the company's website and dedicated training sessions.

3. Introduction to whistleblowing

The term "*whistleblowing*" means reporting wrongdoing or irregularities: (i) that a person internal or external to the entity or company becomes aware of during his or her duties; and (ii) that could harm the entity or company that he or she works for, as well as customers, colleagues, citizens and any other category of subjects.

Sibylla Biotech S.p.A ("**Company**") complies with the ethical principles of honesty, integrity and transparency and with national and international regulations and best practices for its business.

The Company is sensitive to ethical issues and the proper conduct of its business and has therefore implemented its own reporting system to allow the persons identified by law (i.e., Whistleblowers) to report violations of national or European Union regulatory provisions: (i) that harm the public interest or the integrity of the public administration or private entity; and (ii) that they become aware of in a public or private work context, including violations of the Code of Ethics or the Organisation, Management and Control Model under Legislative Decree 231/01 ("**231 Model**").

4. Subject of Reports

There is no exhaustive list of offences or irregularities that could form the subject of a Report. In general, the Report might concern any of the following types of actions or omissions that are committed or attempted:

- criminal, civil, administrative or accounting offences;
- offences that involve legal representatives, directors, managers and/or employees of the Company, *joint ventures* or - in any case - anyone acting on behalf of the Company (e.g. consultants, suppliers, etc.);
- conduct that breaches the 231 Model, the Code of Ethics or other sanctionable company policies or procedures;
- action likely to damage the Company's financial position or reputation;
- potential conflicts of interest;
- actions likely to harm the health or safety of employees or the environment; or
- actions likely to breach the rules introduced to, among other things, protect the following sectors:
    - financial services, products and markets and the prevention of money laundering and terrorist financing;
    - safety and conformity of products;
    - environmental protection;
    - food and feed safety and animal health and welfare;

- public health;
- privacy and data protection and network and information system security; or
- in general, national or European legislation.

In any case, the Whistleblower must have a well-founded reason to believe that the information on the reported violations was true when filing the Report. However, a Report that is manifestly unfounded or defamatory amounts to a breach of this document and attracts possible disciplinary measures and imposes liability on the Whistleblower.

Additionally, Reports must not concern disputes, claims or requests that: (i) are linked to a personal interest of the reporting person or the person filing a complaint with the judicial or accounting authorities; and (ii) relates exclusively to his or her individual employment relationships, or is inherent to his or her employment relationships with hierarchically superior figures or colleagues.

5. Content of Reports

The Whistleblowers must provide all information and evidence to enable the competent functions to check, verify and assess the validity of the facts reported. The Report must therefore be circumstantiated and as complete and exhaustive as possible.

To this end, the Report must contain the following elements:

a. a clear and complete description of the facts that are the subject of the Report;

b. the circumstances of time and place in which they were committed;

c. personal details or other elements enabling the identification of the person(s) who has/have carried out the reported facts (e.g. job title, place of employment where he/she carries out the activity);

c. an indication of any other persons who report any information that forms the subject of the Report;

d. the annexation of any documentation that could confirm these facts; and

e. any other information that could provide useful feedback on the existence of the reported facts.

This is without prejudice to the requirement that the facts or situations reported must be considered true to protect the reported person.

6. Reporting Categories

The following categories of Whistleblowers have the right to file Reports and benefit from the protections provided by the Whistleblowing Law:

a. employees;

b. the self-employed and collaborators (incl. volunteers and trainees);

c. the workers or collaborators of suppliers;

d. freelancers and consultants;

e. directors and members of supervisory bodies; and

f. shareholders.

Additionally, the protections guaranteed to the categories of Whistleblowers listed above also apply if the Whistleblowing occurs:

a. when the legal relationship has not yet begun, if information on violations was acquired during the selection process or at other pre-contractual stages;

b. during the probationary period; and

c. after the termination of the legal relationship, if the information on violations was acquired in the course of that relationship.

Finally, these protections also extend to the following persons:

a. facilitators;

b. persons in the same work environment as the reporting person who are linked to him/her by a stable emotional or family relationship up to the fourth degree;

c. the reporting person's work colleagues who work in the same work environment as the reporting person and who have a regular and current relationship with that person; and

d. entities that the reporting person works for or owns or that operate in the same work environment as that person.

7. The protections guaranteed by the Company

In accordance with the regulations in force, the Company has set up various mechanisms to ensure, throughout the entire process of handling Reports:

a. the confidentiality of the reporter's identity and information;

b. the prohibition of retaliatory or discriminatory acts against the Whistleblower; and

c. the protection of the reported person.

a. Confidentiality of the reporter's identity and information

The Company guarantees the confidentiality of the identities of Whistleblowers and the confidentiality of the information in Whistleblowers' Reports at every stage of the management process, to the extent that anonymity and confidentiality are enforceable under the law.

More specifically, the duty of confidentiality is waived in cases where:

(i) in disciplinary proceedings, the charge is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is indispensable for the accused's defence; and

(ii) the disclosure of the Whistleblower's identity and information that infers the whistleblower's identity, directly or indirectly, is also indispensable for the defence of the person concerned.

In these cases, the reporting person must be notified in writing of the reasons for the disclosure of the confidential data.

Also, the Reports are exempt from the right of access envisaged, and to the extent applicable to the private sector, by Art. 22-*et seq*. of Law 241/1990 and Art. 5-*et seq*. of Legislative Decree 33/2013.

Measures to protect the confidentiality of the Whistleblower are aimed at, among other things, ensuring that the Whistleblower is not subject to any form of retaliation.

b. The prohibition of discrimination against the reporter

The Company prohibits any form of retaliation or discrimination, whether active or omissive, even if only attempted or threatened, carried out due to the Report and that causes or could cause the Whistleblower, directly or indirectly, unjust damage; this protection is guaranteed if the Report (even if subsequently assessed as unfounded) was filed in good faith because the Whistleblower

had reasonable grounds to believe that the information on the reported breaches was true at the time of the Report and that it fell within the objective scope of § 4.

Discriminatory measures are unjustified disciplinary actions, harassment in the workplace or any other form of retaliation that results in intolerable working conditions for the reporting party.[1]

Retaliatory or discriminatory action taken against the Whistleblower could lead to disciplinary proceedings against the perpetrator and disciplinary measures taken in accordance with applicable national labour laws.

Also, a Whistleblower who believes he/she has suffered retaliation/discrimination may take legal action against the author of the retaliation/discrimination and also against the company if he/she actively participated in the act. In this case, the reverses the burden of proof and places the obligation on the company to prove that the Whistleblower's working conditions were not changed because of the decision to file a Whistleblowing report.

A Whistleblower who believes that he/she has suffered retaliation/discrimination for having filed a Report should file a new Report concerning the retaliation/discrimination suffered. The Company must ensure that investigations are carried out promptly in these cases.

c. Protection of the reported person

The Company protects reported persons regarding both the confidentiality of the reports concerning them and any investigations carried out, and the protection of these individuals from any retaliatory and/or defamatory action.

8. The signalling system

The Company's whistleblowing system comprises two channels, written and oral, which reside on the *My Whistleblowing* web platform, accessible at the following link [●].

The Company has equipped itself with this web platform, which is specifically designed to guarantee ease of use, privacy and confidentiality to the reporter. Indeed:

[1] For example:

- dismissal, suspension or equivalent measures;
- relegation in grade or non-promotion;
- change of duties, change of workplace, reduction of salary, or change of working hours;
- suspension of training or any restriction of access to it;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanctions, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- the failure to convert a fixed-term employment contract into an employment contract with an indefinite term, where the employee had a legitimate expectation of the conversion;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- inclusion in improper lists based on a formal or informal sectoral or industry agreement that results in the person being unable to find employment in the same industry in future;
- early termination or cancellation of the contract for the supply of goods or services;
- cancellation of a licence or permit; and
- a request to undergo psychiatric or medical examinations.

1. the use of channels other than the web platform cannot guarantee the same level of protection of Whistleblowers and efficiency in the handling of Whistleblowers; and

2. in the case of anonymous reporting, the web platform allows you to ask the reporter for clarification, while preserving his or her anonymity.

In fact, the Company may also consider anonymous Reports if these have been adequately evidenced[2] and contain extensive information, i.e., they provide facts and illustrate situations that are related to specific contexts (such as documentary evidence, lists of particular names or qualifications, descriptions of specific offices, proceedings or particular events, etc.).

Anyone who receives a Report through channels other than the web platform must forward it within 7 days from receipt to the System Administrator, who must enter it into the web platform and notify the Reporting Party.

In any case, to protect the Whistleblower's privacy without exposing the Company to possible violations of the GDPR, no Reports should be filed by using contacts, computer devices, telephone equipment and/or company networks.

Through the IT channel, the reporter will be guided through each stage of the reporting process and, to better substantiate the report, will have to provide specific information by compulsorily filling in a number of fields.

9. The Reporting Process

The reporting process consists of the following steps:

a. authentication in the web platform, submission of the Report and protocol;

b. taking charge;

c. investigation;

d. decision;

e. archiving and traceability; and

f. information to the reported.

a. Authentication in the web platform, submission of the Report and registration

The reporter first accesses the web platform via the dedicated link.

The web platform will then ask the reporter to authenticate using the access credentials previously received.

The web platform also enables anonymous reporting. Both reporting methods guarantee confidentiality, privacy and protection for the reporter.

Once authenticated, the reporter reports the violation discovered by filling in all the required fields and providing a precise description of the facts and persons involved, as well as attaching any supporting documentation.

The web platform also allows the reporter to submit an Oral Report, simply by choosing the option in the menu sidebar and recording the voice message, which cannot exceed five minutes. After playing back the message, the reporter can then send it in the form of an Oral Report, which

[2] A report can be considered circumstantiated if it allows the identification of factual elements that are reasonably sufficient to initiate an investigation (e.g.: the offence committed, the reference period and possibly the value, the causes and purpose of the offence, the company/division concerned, the persons/units involved, and the anomaly in the control system).

will be stored permanently in the web platform database, ready to be assessed by the System Administrator.

The web platform facilitates interaction with the reporting person and requests for clarification from him/her, while ensuring maximum protection and confidentiality and protection from retaliatory and/or defamatory action.

Upon receipt of the Report, the web platform sends an initial notice confirming receipt and acceptance of the Report and notifies the System Administrator of its entry.

Once the Report is uploaded:

i. The reporter can check the Report's progress at any time by accessing the web platform; and

ii. the System Administrator may continue engaging confidentially with the Reporting Party via the web platform and request further details if the Report is inadequately substantiated.

In light of the above, the reporter should periodically access the web platform to check for any requests for clarification on the report submitted.

b. Taking charge

Upon receipt of the Report, the web platform sends an acknowledgement of receipt of a new Report to the System Administrator's email address.

Upon receipt, the System Administrator carries out a preliminary assessment and classifies the Report based on its characteristics.

In the case of an Oral Report submitted via the web platform, the Manager listens to the message and prepares a summary report of the information shared in written form. Once the summary report has been created, the Oral Report will be displayed on the Manager's dashboard, highlighted with an immediately recognisable graphic sign, and managed in the same way as Written Reports.

At this stage, the System Administrator immediately archives Reports that are manifestly unfounded, instrumental or outside the scope of this procedure.

If , a potential conflict of interest arises when handling the Report, the System Administrator must not proceed with filing the Report and must therefore inform the Reporting Committee to adopt the measures appropriate to ensure proper handling of the Report.

c. Investigation

The System Administrator verifies whether Alerts that have not been immediately discarded provide sufficient information to assess their validity.

If the Report is not manifestly unfounded, instrumental or outside the scope of this procedure but is insufficiently detailed, the System Administrator must issue the appropriate requests for additional information/clarification to the Reporting Party.

After making this initial assessment and obtaining the required clarification and information, the System Operator decides whether to:

i. file Alerts that, following preliminary examination, prove to be unfounded and/or inadequately documented, despite clarification obtained; or

ii. for those Reports that, following the initial assessment, are reasonably well-founded and supported by sufficient information to proceed with the preliminary investigation phase: (a) classifies the Report based on its nature using the categories available on the platform; (b) performs the preliminary assessment; and (c) informs the Reporting Committee of the need to proceed with the preliminary investigation phase.

The preliminary investigation is the set of activities to verify the content of the Reports received and acquire information required for the subsequent decision, guaranteeing the utmost confidentiality of the identity of the Reporting Party and the subject of the Report. The main

purpose of the preliminary investigation is therefore to verify the truthfulness of the information under investigation, through audit procedures and objective investigative techniques.

If the Whistleblowing Committee decides to proceed with the investigation, it prepares a specific investigation plan that covers:

- how the investigation is carried out (requests for additional information/clarification from the reporter, conduct of the investigations considered necessary, etc.);
- the functions, internal or external to the Company, in charge of conducting investigations;
- the functions that could be affected by the violation, based on the subject matter;
- any other persons who might report on the reported facts, whose hearing must be conducted in compliance with the principles of impartiality, confidentiality and protection of the reporter's identity; and
- the timeframe for completing the investigation.

It is everyone's duty to cooperate with all persons in charge of carrying out the investigation. The investigation phase must be completed within 60 days from receiving the Report – except in cases where Reports concerning particularly complex situations require a longer assessment period – in compliance with the principles of impartiality, competence and professional diligence.

During the investigation, if disclosure of the Whistleblower's identity is essential for the defence of the person reported, the Company must tell the Whistleblower why confidential data has been disclosed and request the Whistleblower's consent to disclose his/her personal data.

d. Decision

When the investigation/investigation phase ends, the Reporting Committee files a report with the System Administrator on the outcome of the investigations carried out that contains:

- the established facts;
- the evidence gathered; and
- the causes and shortcomings that allowed the reported situation to occur.

After assessing the results, the Reporting Committee: (i) expresses its decision on the Report; (ii) identifies – in consultation with the CEO[3] – the possible disciplinary measures and corrective action to be proposed; and (iii) instructs the System Administrator on the feedback to be provided to the Reporting Officer.

In any case, the feedback to the Reporting Party on the outcome of the relevant Report must be provided within 3 months from acknowledgement of receipt of the Report, or – without this notice – within 3 months from expiry of the 7-day period for such notice. If the investigation has not been concluded by virtue of facts that require, for verification purposes, more than 3 months, the Reporting Party must in any case be provided an interim reply by expiry of the deadline indicated.

Disciplinary measures

Disciplinary measures must be appropriate and proportionate to the breach ascertained, also considering the possible criminal relevance of the conduct, and must comply with the provisions of applicable national labour laws.

The disciplinary measures proposed following the establishment of the breach must be shared with the functions affected by the breach. The measures are then finally approved and adopted by

[3] If the report concerns conduct referable to the CEO, the decision will be taken in consultation with the Board of Directors (excl. the CEO).

the CEO[4] and are communicated to the person responsible for the violation, in compliance with applicable national labour laws.

Corrective Measures

The Reporting Committee shares with the corporate functions affected by the violation the appropriate corrective measures to remedy the consequences of the violation and to prevent the risk of violations similar to the violation(s) reported.

The functions concerned by the breach must confirm the implementation of the measures identified and inform the Reporting Committee of their outcome. The Whistleblowings Committee informs the System Administrator of the implementation of the corrective measures in order to follow up with the Whistleblower.

e. Archiving and traceability

In order to ensure traceability, confidentiality, preservation and retrievability of data throughout the process, the Reports received (together with any attached documentation) are stored and archived in digital format on the web platform.

All documentation must be kept for as long as necessary for processing the Report and in any case max. five years from the date of the communication of the final outcome of the reporting procedure.

In any case, personal data related to Reports are processed in accordance with Regulation (EU) 2016/679, Legislative Decrees 196/2003 and 51/2018 and therefore personal data that is manifestly not needed for processing a specific Report are not collected or, if accidentally collected, are deleted immediately.

f. Information to the reported

During all phases of handling Reports, the Reporting Committee considers how to inform the reported person of the transmission of the Report against him/her, the conduct of the related investigation and its outcome.

More specifically, the reported person must be informed of the Report against him/her and that it must be assessed on a case-by-case basis by checking whether sending the report could prejudice the conduct of the investigations necessary to ascertain the facts that are the subject of the Report or whether, on the contrary, the involvement of the reported person is necessary for development of the investigation.

The Company guarantees, in any case, a right for the reported person to be able to defend himself/herself and to be informed (within a reasonable time) of the charges and of any disciplinary measures against him/her.

10. **Reporting**

The System Administrator prepares at one report per year on all Reports received and managed, which it must forward to the company's management and control bodies.

In any case, the System Administrator, at any stage in the process of handling a Report, may inform the company's management and control bodies of any Reports that could materially impact the Company.

[4] See previous footnote.

11. **External signalling**

Whereas, as illustrated in this document, the Company has set up appropriate internal reporting channels, in compliance with the provisions of the Whistleblowing Law, Whistleblowing is allowed through the external channel activated by the National Anticorruption Authority ("**ANAC**") only if the Whistleblower has:

(i) already filed an Internal Report that was not followed up on;

(ii) reasonable grounds exist to believe that, if it were to file an internal report, the report would not be effectively followed up or the report itself might lead to the risk of retaliation; or

(iii) reasonable grounds exist to believe that the breach could constitute an imminent or obvious danger to the public interest.

Without the above prerequisites, the report is not handled by ANAC and the person does not benefit from the protections provided for in the Whistleblowing Law.

The external reporting channel activated by ANAC is available at the following link: https://whistleblowing.anticorruzione.it/#/.

12. **Dissemination and training**

The Company ensures the dissemination of this document to all employees and third parties that have legal relations with it, as well as the organisation of training sessions on the subject. More specifically, the Company provides clear information on the channels, procedures and prerequisites for filing internal Reports, as well as on the channels, procedures and prerequisites for filing external Reports.

This information is published in a dedicated section on the company's website.

The training, addressed to all employees, is carried out regularly and, in any case, whenever the need arises and includes, to the extent possible, case studies and examples aimed at avoiding the recurrence of any situations that have already arisen.

Additionally, new entrants are promptly informed of the rules and procedures to protect employees in the event of whistleblowing.

13. **Infringement of procedure**

Breach of any of these procedures results in the Company's employees being subject to the application of the Company's Disciplinary System, in line with all applicable legislation, collective labour agreements and the 231 Model adopted by the Company.