# PRIVACY POLICY
# in accordance with Arts. 13 and 14 of the European Union Regulation on the Protection of Personal Data

# PRIVACY POLICY

*Dear User,*

*Here at Sibylla Biotech S.p.a. ("**Company**") we need to be informed immediately of any suspected violation or fear of violation of laws, regulations or internal policies and procedures. Reports can be made through various channels, including the digital platform My Whistleblowing ("**Platform**") and the voice mailbox available on the Platform ("**Voice Mailbox**").*

*Regardless of the channel used, the receipt and analysis of a report, as well as any subsequent investigation carried out, will involve the processing of personal data by the Company.*

*The Company takes the protection of personal data seriously and therefore invites you to read the following information notice – drafted in accordance with Legislative Decree 196/2003 (as amended) and EU Regulation 2016/679 on the protection of personal data – which is intended to help you understand how we process and handle the personal data and information contained in the report and to inform you of your rights in this regard.*

*If you have any doubts or questions regarding this policy, please contact the Company at the following* email *address: contact@sibyllabiotech.it*

We provide you with this information in accordance with Arts. 13 and 14 of the European Data Protection Regulation 679/2016 ("**GDPR**") and Legislative Decree 196/2003 of the Personal Data Protection Code ("**Privacy Code**") .

**THE DATA CONTROLLER.**

The data controller is **Sibylla Biotech S.p.A.** with registered office in Bresso (MI), Via Lillo Del Duca 10, email: sibyllabiotech@legalmail.it

**PLACE OF DATA PROCESSING**

Related processing takes place in Italy and no data is transferred or disseminated abroad or to non-EU countries. Data is communicated or disseminated only for statistical purposes in an anonymous and/or aggregate way.

**PURPOSE OF DATA PROCESSING**

The personal data you provide is used for the sole purpose of handling your Whistleblowing report and is processed only to:

- manage the life cycle of the alert, carrying out investigations with the parties concerned (incl. public authorities);
- enable the management of the platform and related reports;
- determine whether a tort has occurred;
- determine the relevant penalties and any mitigating measures to be put in place to prevent future wrongdoing;
- verify and ensure the correct and complete application of company policies and to implement any activity subsequent and consequent to such verifications, and to comply with specific legal obligations, regulations and applicable legislation regarding the Company's internal control and monitoring of corporate risks specifically required by law; and
- carry out statistics and reports.

**PROCESSED DATA**

Personal Data is any information relating to an identified or identifiable natural person ("data subject").

If the User decides to file a report, the following categories of data may be processed within the framework of the handling of reports by the Data Controller:

i. user identification data: first name, last name and contact information;

ii. Personal Data of the reported person or other parties mentioned, or data obtained by the Data Controller during the investigation: name, surname and Personal Data (e.g., job description and contact information); and

iii. information related to the reported breach: description of the alleged breach, as well as a description of the circumstances of the case, or other information obtained during the investigation of the reported facts, records/resumes of the investigation process, and actions taken as a result of the investigation.

The information in some reports can include special categories of Personal Data.

Under Art. 9 of the GDPR, data that could reveal racial or ethnic origin, religious or philosophical beliefs, political opinions, party or trade union membership, data concerning health and sexual orientation or criminal proceedings is considered 'special data'.

The GDPR imposes stricter restrictions for this type of data, which may be processed only if and when it is relevant to the reporting and only to the extent permitted by applicable law and/or the need to ascertain, exercise or defend a right in an action pending before a court under Art. 9(2)(f) of the GDPR. However, if this data is not relevant for reporting and is outside the scope permitted by the applicable law and/or is not necessary for establishing, exercising or defending a right in an action

pending before a court of law, it must be promptly and securely deleted and may not be processed any further.

**LEGAL BASIS FOR PROCESSING**

Personal Data may be processed for purposes of a compulsory nature related to compliance with applicable laws and regulations and to comply with any requests received from competent Authorities.

Legitimate interest is also a legal basis and the Company will also retain Personal Data based on the Company's legitimate interest in properly handling all reports it receives – in line with the relevant Policy for Handling Reports – in order to prevent and investigate the alleged violations set out in the policy and to defend its rights in (or bring) legal proceedings accordingly.

The Personal Data of the User and of all persons mentioned in the report may be processed without the relevant consent in cases where this is necessary to pursue the legitimate interest of the Data Controller in receiving and processing reports of actual or alleged violations of laws or regulations applicable to the Companies, as well as of internal policies and procedures.

The processing of data must in any case be carried out in accordance with all applicable principles of purpose, relevance, appropriateness and limitation.

**STORAGE TIMES**

Your personal data will be processed and stored by the Data Controller for the time strictly required to manage your report in line with all needs that arise when assessing your report (e.g., legal case and proceedings before public authorities) or fulfilling legal obligations. In any case, all data you provide will be deleted from the Platform within 5 years from closing the investigation, unless the Data Controller is obliged to continue storing it in order to fulfil legal obligations or to ensure the possibility of legal defence. However, in this case your data will not be subject to any further processing

If any checks carried out in connection with the report produce no evidence of a breach (unfounded report) or if the report falls outside the scope of the reportable conduct (irrelevant report), the Personal Data relating to the report will be deleted immediately.

When this time limit expires, Personal Data will be deleted or anonymised in accordance with our internal procedures, unless otherwise required by law or if the Personal Data is necessary to protect our rights before any judicial or other competent authority.

We also inform you that, under Arts. 5 and 89.1 of the GDPR, Personal Data may be stored in anonymous form for longer periods than those specified in the

preceding paragraph for statistical purposes only, subject to the implementation of appropriate technical and organisational measures necessary to protect your rights and freedoms.

**WITH WHOM WE SHARE THE COLLECTED DATA**

Your Personal Data may be accessed **within the Company** by the employees in charge of investigating Whistleblowing Reports and by the manager of the Whistleblowing Reporting System. Additionally, given that Whistleblowing reports are submitted through the My Whistleblowing software application, your Personal Data may also be accessed by the provider of the above application, who has been appointed as data processor for this purpose under Art. 28 of the GDPR.

Additionally, Personal Data may be shared with third-party companies or individuals who perform instrumental activities on behalf of the Company, such as Platform Suppliers and External Consultants. These individuals serve as Data Processors and under the direction and monitoring of the Company.

In any case, the report will only be processed by specifically appointed, autonomous, dedicated and specifically trained internal or external personnel, also regarding the constraints imposed by Personal Data Protection legislation, based on a need-to-know principle envisaged by the GDPR.

The protection of Personal Data and the legitimacy of the processing is guaranteed by the appropriate appointment as Data Processors of all third parties who carry out processing in the name and on behalf of the Company. All our Data Processors are therefore required to comply with applicable privacy laws and to implement adequate security measures.

Also – again for the purposes strictly instrumental for assessing reports and implementing legal or contractual provisions – in some circumstances the Company may need to transmit, directly or indirectly, some of the Personal Data contained in the report – based on a strict relevance criterion – outside the Company to the following categories of subjects:

i. public security authority; and

ii. judicial authorities.

These parties will serve as (autonomous) Data Controllers (of the respective processing operations), unless they serve on behalf of the Company as Data Processors and have therefore entered into a specific contract governing the processing entrusted to them, in accordance with Art. 28 of the GDPR.

The identity of the User, serving as a reporting individual, will only be disclosed if required by laws or regulations or a previously issued request for disclosure, or to ensure the reported individual's right to file a defence, where the reporting individual has given his or her consent.

It is understood that, in line with the principle of protecting the confidentiality of the reporter as set out in Legislative Decree 24/2023, sharing your personal data is limited to purposes that are strictly necessary to guarantee your confidentiality.

**MODE OF TREATMENT**

Personal data is processed both by automated and manual means and for the purposes indicated above. Specific security measures are observed to prevent loss of data, unlawful or incorrect use and unauthorised access.

The Personal Data provided will be processed by the Company in accordance with the methods and in compliance with the legislation in force, in accordance with the principle of minimisation and through methods suitable to guarantee their security and confidentiality. More specifically, processing this data will be carried out:

- via a digital or audio medium, depending on the channel used for signalling; or
- in a way that ensures the highest standards of confidentiality and to prevent or minimise the risks of destruction or loss (incl. accidental) of any data, or unauthorised access or processing of data that is not permitted or not in accordance with the purposes of collection.

In accordance with the GDPR, Personal Data obtained from time to time may be used to update and correct previously collected information.

In order to guarantee the confidentiality of the whistleblower for the entire duration of the handling of the internal report, a Whistleblower's identity will be revealed only to those persons expressly authorised to handle reports. Every Whistleblower's identity is protected in any context after filing the report and cannot be revealed without his/her express consent, and all those who receive or are involved in managing the report are required to protect the confidentiality of such information.

**RIGHTS OF THE INTERESTED PARTIES**

Under certain conditions, you have the right to exercise the rights envisaged under Arts. 7, 8, 9 and 10 of the Privacy Code and Arts. 15, 16, 17, 18, 19, 20, 21 and 22 of the GDPR and, in particular, to request:

- access to your personal data;
- a copy of all personal data you have provided us with (i.e., 'portability');
- rectification of all data in our possession;
- deletion of any data that we no longer have any legal requirement for processing;
- opposition to processing where provided for by applicable law;
- revocation of your consent, if the processing is based on consent; and
- restriction on how we process your personal data, within the limits envisaged by data protection legislation.

The ability to exercise of these rights is subject to certain exceptions aimed at safeguarding the public interest (e.g., prevention or identification of crimes) and our interests (e.g., maintaining professional secrecy). If you exercise any of the above rights, we are required to verify that you are entitled to exercise them and we will, as a rule, reply to you within one month.

Anyone who requires further clarification on compliance with the privacy policy adopted by Sibylla Biotech S.p.A., its application, the accuracy of their personal data or the use of the information collected, may contact us by email at: contact@sibyllabiotech.it

However, if you prefer, you may forward any complaints or reports, in accordance with Art. 77 of the GDPR, to the data protection authority directly using the following contact details:

**Post**: Garante per la protezione dei dati personali - Piazza di Monte Citorio n. 121 - 00186 ROMA

**Fax**: (+39) 06.69677.3785 **Telephone**: (+39) 06.696771

Email: garante@gpdp.it Certified email: protocollo@pec.gpdp.it