APTUIT (VERONA) S.R.L.

Whistleblowing Policy for the management of reportings and the protection of the whistleblower

INTRODUCTION

This Policy is adopted by the Company Aptuit (Verona) Srl ("Aptuit" or the "Company") in order to regulate the receipt and management of whistleblowing reportings directed to the body appointed by Evotec Group, in compliance with confidentiality obligations and any other prescription imposed by Legislative Decree no. 24 of 10 March 2023, by the ANAC Guidelines and following the operational guide developed by Confindustria.

This Policy integrates the local "Whistleblowing system" adopted by the Company together with the "*Whistleblowing Policy for sending/receiving reportings and the protection of the whistleblower*" and the Evotec Group Policy "Global Whistleblowing and Case Handling Policy" which are intended here to be referred to in full.

1. WHO CAN REPORT THROUGH INTERNAL REPORTING SYSTEMS

The following categories of subjects can make a reporting:

- Employees o Collaborators o Suppliers, subcontractors and employees and collaborators of the same
- Freelancers, consultants, self-employed o Volunteers and trainees, paid or unpaid
- Shareholders or persons with administrative, managerial, supervisory or representative functions
- Former employees, former contractors, or persons who no longer hold any of the positions mentioned above
- Subjects in the selection phase, on trial or whose legal relationship with the institution has not yet begun.

2. WHAT KIND OF WRONGDOING CAN BE CONSIDERED IN REPORTING PROCEDURES

Unlawful acts of which one has become aware in the context of one's work may be reported. Suspected or qualified offences or other violations of legal provisions or potential risks of committing them may also be reported. The reporting person is not required to fully prove the commission of an offence but the reportings must be as detailed as possible, in order to allow an assessment of the facts communicated by the recipients.

Reportings may concern:

- **relevant offences pursuant to Legislative Decree no. 231/01 or violations of Organisational Model 231 or the Code of Conduct;**
- **offences falling within the scope of European Union or national acts, or national acts** implementing European Union acts, relating to the following areas: public procurement, services, financial products and markets and the prevention of money laundering and terrorist financing, product safety and compliance, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety and animal health and welfare; public health, consumer protection; protection of privacy and protection of personal data and security of networks and information systems;
- **acts or omissions affecting the financial interests of the European Union;**
- **acts or omissions relating to the internal market, including infringements of EU competition and State aid rules, as well as infringements concerning the internal market related to acts infringing corporate tax rules or mechanisms the purpose of which is to obtain a tax advantage which defeats the object or purpose of the applicable corporate tax legislation;**
- **acts or conduct which defeat the object or purpose of the provisions of Union acts in those areas;**
- **violations in the field of whistleblowing** (violation of confidentiality obligations regarding the identity of the whistleblower; violation of the prohibition of retaliatory or discriminatory acts against the whistleblower; obstructing or attempting to obstruct a reporting; failure to establish, having been entrusted with them, the reporting channels or procedures for making and managing reportings or adopting procedures that do not comply with those referred to in articles 4 and 5 of Legislative Decree 24/2023; not having reported to the Surveillance Body (SB) the information flows on whistleblowing and disciplinary measures adopted; ascertainment, also by means of a first instance judgment, of the criminal liability of the whistleblower for the crimes of defamation or slander or in the event that such crimes are committed by reporting to the judicial or accounting

authorities; ascertainment of civil liability for the same reason for wilful misconduct or gross negligence).

By way of example and not limited to, the reporting may concern:

- Offences pursuant to Legislative Decree 231/2001 (corruption, corporate crimes, tax offences, undue receipt of public disbursements, promise or giving of money, goods or services or other benefits aimed at bribing suppliers or customers);
- offences relating to the following sectors: public contracts; financial services, products and markets and the prevention of money laundering and terrorist financing; safety conformity of products; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems. By way of example, the so called environmental crimes, such as the discharge, emission or other release of hazardous materials into the air, soil or water, or the illegal collection, transport, recovery or disposal of hazardous waste;
- fraud, corruption and any other illegal activity related to Union expenditure;
- and infringements of EU competition and state aid rules, corporate tax and mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax legislation;
- abusive practices (adoption of so-called predatory prices, target discounts, tying) in contravention of the protection of free competition
- Offences relating to the environment and the health and safety of workers;
- Unlawful use of personal data or blatant violations of privacy regulations.

The subject matter of this procedure does not include reportings of a personal nature that do not affect a general interest, for example relating to one's employment contract, which are governed by other procedures of the institution.

It will not be possible to manage reportings relating to areas other than those listed in paragraph 3 above with the protections provided for by the whistleblowing legislation: the whistleblower will be invited to forward the reporting to the correct channel or the reporting will be treated as ordinary.

3. REPORTING CHANNELS

The Company makes available to reporting individuals the following tools for reporting violations under this procedure. In particular, it is possible to make oral and written reportings.

a. **With regard to written and oral reportings via voice messaging**, the entity shall make available the **encrypted IT platform "EQS Integrity Line" (already known to the Evotec**

Group as "EVOWhistle" which can be accessed through the link https://evotecgroup.integrityline.org and which is available also in the dedicated Evotec internet page: https://www.evotec.com/en/investor-relations/governance - **section "REPORTING COMPLIANCE VIOLATIONS"**. This tool guarantees, from a technological point of view, the confidentiality of the reporting person, the persons mentioned in the reporting and the content of the same. A menu in the platform guides the whistleblower in the reporting path. It is also possible to attach documents. The system attributes a code to the reporting. The Whistleblower can access the reporting and communicate bidirectionally with the recipient, exchange messages and send new information.

All information contained on the platform is encrypted and can only be read by persons authorized to receive the report.

It is not possible to manage other written reportings. If these are sent, the receiving party will, where possible, invite the reporting person to resubmit the reporting via the IT platform.

b. **For reportings by face-to-face meeting**, the whistleblower may contact the **receiving entity through the IT platform, requesting availability for a personal meeting, including via videoconference**. Reports made in a personal meeting are recorded by the reporting manager and countersigned by the whistleblower (who receives a copy) and by the manager himself. The report is then uploaded to the IT platform in the presence of the whistleblower who will be able to obtain the access keys to check the status of the report.

For reports via recorded voice messaging or recorded face-to-face meeting, the whistleblower will issue prior informed consent to the processing of data.

4. THE REPORTING MANAGER

The Company has identified an internal reporting channel and, as Managing Body, an "Ethics Committee" composed of the Legal Counsel and internal member of the Surveillance Body of the Company with a second or third member whose identification is, at the time of drafting this Policy, being defined, which will be subject to a specific written appointment.

These subjects are endowed with autonomy and specifically and adequately trained in the management of reports, in order to ensure that they are managed in an adequate manner and in compliance with the provisions of the Decree. In particular, this requirement must be understood as:

- Impartiality: lack of bias and bias towards the parties involved in whistleblowing reports, in order to ensure fair management of reports free from internal or external influences that may compromise their objectivity;
- Independence: autonomy and freedom from influence or interference by management, in order to ensure an objective and impartial analysis of the report.
- Autonomy of expenditure with allocation of budget in case of the need to make use of external consultants.

5. CONFIDENTIALITY

a. In the management of the reporting

The recipient is obliged to treat the reports while preserving their confidentiality. Information relating to the identity of the reporting party, the reported person and any other person mentioned in the report shall be treated in accordance with the principles of confidentiality. In the same way, all information contained in the report is also treated confidentially. The identity of the reporting person may not be revealed without their consent. Knowledge of the reports and the related acts of assessment are also removed from the right to administrative access by the interested parties. The only possible ground for revealing the identity of the reporting person may occur if the assessment documents are forwarded to an ordinary or accounting prosecutor's office and knowledge of the same is necessary for the purposes of the right of defence during ordinary judicial or accounting proceedings at the Court of Auditors. Confidentiality is guaranteed through the tool of the encrypted IT platform and within organizational processes aimed at minimizing the circulation of information.

These protection measures apply not only to the reporting entity but also to other entities that could be subject to retaliation, due to the role assumed or the particular proximity or relationship with the whistleblower. In particular, these are the following subjects:

- **facilitator**, i.e. the natural person who assists the whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential;
- **persons in the same working context as the whistleblower** and who are linked to them by a stable emotional or family bond within the fourth degree. On the notion of "stable emotional bond", the ANAC guidelines provide that "this expression could refer, first of all, to those who have a cohabitation relationship with the whistleblower and precisely: work colleagues of the whistleblower, complainant or of those who make a public disclosure, who work in the same work context as the same and who have a habitual and current relationship with said person.
- entities owned - exclusively or **majority-owned** by third parties - of the whistleblower, complainant or public disclosure;
- **entities where the whistleblower, complainant or public disclosure person works.**

For the correct identification of such subjects, also for the purpose of guaranteeing confidentiality and the protections granted to them, as part of the process of investigation of the report, the whistleblower explicitly indicates the existence of such subjects, demonstrating the existence of the relevant conditions.

b. <u>In disciplinary proceedings</u>

In the context of the disciplinary proceedings initiated by the entity against the alleged perpetrator of the reported conduct, the identity of the whistleblower cannot be revealed, if the objection to the disciplinary charge is based on separate and additional investigations with respect to the report, even if consequent to the same. If, on the other hand, the complaint is based, in whole or in part, on the report and the identity of the whistleblower is indispensable for the defence of the person to whom the disciplinary charge has been charged or of the person involved in the report, the latter will be used for the purposes of the disciplinary proceedings only with the express consent of the reporting person to the disclosure of his or her identity. In such cases, prior notice shall be given to the reporting person by means of written communication of the reasons that make it necessary to disclose the confidential data. If the reporting party denies his/her consent, the report cannot be used in the disciplinary proceedings which, therefore, cannot be initiated or continued in the absence of further elements on which to base the complaint. In any case, the right of the entity to proceed with the complaint to the judicial authority remains unaffected, provided the conditions are met.

6. WHISTLEBLOWING ACTIVITIES

6.1 Written submissions

The whistleblowing manager receives and archives the reports through the IT platform and, again through the same, dialogues with the reporting person to clarify and deepen what has been received. The dialogue continues even during the assessment phases. After an initial assessment, it carries out an activity of verification of the information reported, also requesting specific information from other offices and functions within the organization. The recipient provides periodic feedback to the reporting person and, at the end of the investigation (within 3 months from the acknowledgement of receipt of the report), communicates the outcome of the investigation activities. The communication of the outcome does not include references to personal data relating to any reported subject. Among the possible outcomes that can be communicated to the reporting person are:

- Correction of internal processes
- Initiation of disciplinary proceedings
- Transfer of the results of the investigation activities to the Public Prosecutor's Office
- Archiving due to lack of evidence

6.2 Oral reportings

a. In the case of reporting with voice messaging through the IT platform, what is described in point 3 applies, it being understood that pursuant to Article 14 of Legislative Decree 24/2023, the manager will collect the informed consent of the whistleblower in advance to the processing of personal data.
b. In the case of a face-to-face meeting, the reporting manager must ensure that the meeting takes place within 15 days.The meeting must take place in a suitable place to guarantee the confidentiality of the whistleblower (e.g. office of the Surveillance Body). A report will be made by the manager of the reports, it being understood that pursuant to art. 14 of Legislative Decree 24/2023, the manager will collect the whistleblower's informed consent in advance to the processing of personal data. The report will be countersigned by the whistleblower (who receives a copy) and by the manager himself. The reports made in person are then uploaded to the IT platform in the presence of the whistleblower who will be able to obtain the access keys to check the status of the report.

6.3 Receipt of the report and response time

Through the tools of the IT platform, the manager of the report issues to the whistleblower the notice of mere receipt of the same within **7 days** from the submission of the report itself. This notice must be sent to the address indicated by the whistleblower in the report. In the absence of such an indication, the whistleblower will be able to independently access the platform to ascertain the status of the report.

6.4 Conflict of interest

In the event that the report concerns cases in which one of the members of the Whistleblowing Ethics Committee coincides with the whistleblower, with the reported or is in any case a person involved or affected by the report, the report may be addressed to the other member who will be able to guarantee its effective, independent and autonomous management, always in compliance with the obligation of confidentiality provided for by the regulations. If the conflict concerns the entire function of both members, the report may be forwarded to the Chairperson of the Board of Directors, who may ensure its effective, independent and autonomous management, always in compliance with the obligation of confidentiality provided for by the regulations.

6.5 Suspension of Service and Replacements

The whistleblowing service is suspended on Sundays and all public holidays.

the management of reports, he/she will take care to communicate this to the other member so that he/she can take over the reception and management of reports *on an interim* basis until the return of the function

to ensure compliance with the terms provided for by the decree. In the event of prolonged absence of the entire Ethics Committee, the same will take care to communicate it to the Chairperson of the Board of Directors so that he can take over the reception and management of reports *on an interim* basis until the return of the function to ensure compliance with the terms provided for by the decree.

6.6 Anonymous reports

In the case of receipt of anonymous reports, it is specified that the same, if they are punctual, detailed and supported by appropriate documentation, will be equated by the company to ordinary reports and will be processed. In any case, anonymous reports will remain recorded and stored on the IT platform. Where the anonymous whistleblower, even upon solicitation to come forward, is subsequently identified and has suffered retaliation, the whistleblower will be guaranteed the protections provided for the whistleblower.

6.7 Preliminary examination: admissibility and admissibility

Once the phase relating to the transmission of the acknowledgment of receipt has been completed, the operator proceeds with the preliminary examination of the report received, assessing its admissibility and subsequently its admissibility. Below are some evaluations that can be made in these phases.

a. Proceedability.

In order to proceed with the procedure, the reporting manager must, first of all, verify the existence of its conditions and, specifically, that the whistleblower is a person entitled to make the report and that the subject of the report falls within the scope of application of the discipline.

b. Eligibility

Once it has been verified that the report meets the subjective and objective requirements defined by the legislator and, therefore, is prosecutable, it is necessary to assess its admissibility as a whistleblowing report. In order to be eligible, it is necessary that the following are clear in the report:

- the circumstances of time and place in which the fact that is the subject of the report occurred and, therefore, a description of the facts that are the subject of the report, which contains the details relating to the circumstantial information and, if present, also the ways in which the whistleblower became aware of the facts;
- personal details or other elements that make it possible to identify the person to whom the reported facts can be attributed.

In the light of these indications, the report can, therefore, be considered inadmissible for:

- lack of data that constitute the essential elements of the report;

- manifestly unfounded the factual elements attributable to the violations typified by the legislator;
- exposition of facts of generic content such that they cannot be understood by the offices or the person in charge;
- production of documentation only without the actual reporting of violations.

In light of the above, in the event that the report is inadmissible or inadmissible, the offices or the person responsible for managing the report may proceed with the archiving, while still ensuring the traceability of the supporting reasons.

In addition, during the preliminary verification, the persons in charge of managing the report may request from the whistleblower additional elements necessary to carry out in-depth investigations relating to the report.

6.8 Investigation and guarantees of confidentiality in case of external support to the Committee

Once the admissibility and admissibility of the report has been verified, the operator starts the internal investigation into the facts and conduct reported in order to assess their merits. The manager shall ensure that all appropriate checks are carried out on the facts reported, ensuring timeliness and compliance with the principles of objectivity, competence and professional diligence. The objective of the investigation phase is to proceed with specific checks, analyses and assessments of the validity or otherwise of the facts reported, also in order to formulate any recommendations regarding the adoption of the necessary corrective actions on the areas and business processes concerned with a view to strengthening the internal control system. Whistleblowers must ensure that the necessary checks are carried out, including, but not limited to:

- directly acquiring the information necessary for the evaluations through the analysis of the documentation/information received
- through the involvement of other company structures or even external specialized subjects (e.g. IT specialists) in consideration of the specific technical and professional skills required;
- hearing of any internal/external parties, etc.

This investigation and verification activity is the sole responsibility of the persons in charge of handling the reports, including all those activities necessary to follow up on the report (for example, hearings or the acquisition of documents).

In the case of an oral report in presence, the report drawn up must be scanned and stored in the encrypted IT platform.

In case of reports relating to behavior aimed unequivocally at the commission of crimes or if it is necessary to proceed with internal investigation activities, the manager of the report must make use of the technical assistance of a trusted criminal lawyer. In this case and in all those involving the use of specialist support from third-party professionals, as well as from the staff of other company functions/directions, it is necessary - in order to guarantee the confidentiality obligations required by law - to obscure any type of data that could allow the identification of the reporting person or any other person involved (think, for example, of the facilitator or other people mentioned in the report). In the case of involvement of external technical expertise, the reporting manager can have and use the budget approved by the Board of Directors. If the involvement of internal parties other than the Manager (other company functions) is necessary, confidentiality obligations are also extended to them. If the identifying data are necessary for the investigation conducted by external parties (possibly involved by the Manager), it will be necessary to extend the duties of privacy and confidentiality envisaged by the Decree for the Manager also for these external parties through specific contractual clauses to be included in the agreements stipulated with the external party. Furthermore, in both cases, the necessary privacy designations must be ensured.

6.9 Conclusion of the investigation

Once the investigation activity has been completed, the reporting manager can:

- archive the report because it is unfounded, giving reasons for it;
- declare the report to be well-founded and contact the relevant internal bodies/functions for follow-up (e.g. company management, General Manager, legal department or human resources). In fact, the reporting manager is not responsible for any assessment of individual responsibilities and any subsequent consequent measures or proceedings.

  All phases of the investigation activity must always be tracked and archived correctly depending on the type of reporting channel used, in order to demonstrate the correct diligence required in following up on the report.

6.10 Feedback to the whistleblower on the results of the investigation

The reporting manager shall provide a response to the whistleblower within 3 months of the date of acknowledgment of receipt or - in the absence of such a notice - within three **months** of the date of expiry of the seven-day period for such notice. It will not be necessary to complete the assessment within three months, considering that there may be cases that require a longer time for the purposes of verification. Therefore, it is a finding that, at the end of the term indicated, may be definitive if the investigation has been completed or of an interim nature on the progress of the investigation, which has not yet been completed. Therefore, at the end of the three months, the reporting manager may communicate to the whistleblower:

- the filing of the report, justifying the reasons;
- the verification of the validity of the report and its transmission to the competent internal bodies;
- the activity carried out so far and/or the activity he/she intends to carry out. In the latter case, it will be the responsibility of the manager to communicate to the reporting person also the subsequent final outcome of the investigation of the report (archiving or verification of the validity of the report with transmission to the competent bodies).

7. RETENTION OF REPORTING DOCUMENTS

The reports and the related documentation are stored within the encrypted IT platform for the time necessary to process the report and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure. Any analog documentation will be kept by the manager in a special locked archive at its sole disposal.

8. TRAINING AND INFORMATION

The offices or persons responsible for the management of the reporting channel are provided with specific training relating to the management of the channel.

Whistleblowers shall provide the reporting person with clear information about the channel, procedures and conditions for making reports, whether internal or external.

To this end, this "*Whistleblowing Policy for the management of reportings and the protection of the whistleblower*", together with the "*Whistleblowing Policy for sending/receiving reportings and the protection of the whistleblower*" and the whistleblowing reporting platform are available in the dedicated Evotec internet page: https://www.evotec.com/en/investor-relations/governance **- section REPORTING COMPLIANCE VIOLATIONS.**

The IT platform also integrates operational instructions as well as guiding the whistleblower through the reporting process.

This information is also been disclosed to all Aptuit employees via internal communication.

9. MANAGEMENT OF PERSONAL DATA

Any processing of personal data, including communication between competent authorities, must be carried out in accordance with Regulation (EU) 2016/679, Legislative Decree No. 196 of 30 June 2003 and Legislative Decree No. 51 of 18 May 2018. Personal data that is clearly not useful for the processing

of a specific report is not collected or, if collected accidentally, is deleted immediately. The rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised within the limits of the provisions of Article 2-undecies of Legislative Decree No. 196 of 30 June 2003.

The processing of personal data relating to the receipt and management of reports is carried out by the Company in its capacity as data controller, in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679 or Articles 3 and 16 of Legislative Decree no. 51 of 2018, providing appropriate information to reporting persons and persons involved pursuant to Articles 13 and 14 of the same Regulation (EU) 2016/679 or Article 14 of the same Regulation (EU) 2016/679 or Article 14 of the same Regulation (EU) 2016/679 11 of the aforementioned Legislative Decree no. 51 of 2018 as well as adopting appropriate measures to protect the rights and freedoms of data subjects. In the case of oral reporting, pursuant to art. 14 of Legislative Decree 24/2023, the manager will collect the whistleblower's informed consent in advance to the processing of personal data.

A level of security appropriate to the specific risks arising from the processing carried out is guaranteed, on the basis of a data protection impact assessment, and by regulating the relationship with any external providers who process personal data on their behalf pursuant to Article 28 of Regulation (EU) 2016/679 or Article 18 of Legislative Decree No. 51 of 2018.

The personal data relating to the report is only known to the reporting operator. During the assessment activities, the recipient may share with other functions of the entity information that has been previously anonymized and minimized with respect to the specific activities within the competence of the latter.