POLICY AND PROCEDURES FOR MANAGING REPORTS REGARDING VIOLATIONS OF EU LAW

(Whistleblowing)

1η Edition

January 2024

INTRODUCTION

I. REPORTING POLICY

INTRODUCTION

1.1 General – Purpose

ProGnosis Biotech S.A. (hereinafter referred to as the “Company”) is a Greek public limited company operating in the field of biotechnology.
As part of its regulatory compliance, the Company adopts this Whistleblowing Policy for Violations of EU Law (hereinafter: "WPEUL"), while ensuring the establishment and operation of secure reporting channels.
The WPEUL is adapted to the principles and provisions of the European Directive 2019/1937 on the protection of persons who report violations, which was incorporated into national legislation by Law 4990/2022 "Protection of persons who report violations of EU law – Incorporation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 (L 305) and other urgent regulations".
The Company falls under the scope of Law 4990/2022, as it employs more than fifty (50) and fewer than two hundred forty-nine (249) employees. The calculation of the number of employees is made in accordance with Law 4308/2014.
The WPEUL defines the general principles and operational framework under which the Company receives, processes, and investigates reports of violations of EU law, violations affecting the financial interests of the EU under Article 325 of the Treaty on the Functioning of the European Union (TFEU), and violations related to the internal market under Article 26 of the TFEU, in accordance with the provisions of Article 4 of Law 4990/2022, which come to the attention of the personnel and individuals covered under the personal scope of Article 6 of Law 4990/2022.
Through the WPEUL:
• Rules are established to facilitate and encourage the making of named or anonymous reports and complaints related to the above.
• Integrity, transparency, accountability, and the detection of potential violations of the Company's regulatory framework are strengthened.
• Appropriate and necessary measures are adopted to prevent or address potential incidents, with the aim of protecting the Company's reputation and its employees.

The approval of the WPEUL and any amendments to it are made by the Company’s Board of Directors.
The WPEUL is communicated to all Company personnel (regardless of their employment/engagement relationship), so they are informed, and it is posted on the Company's intranet so that every employee has immediate and continuous access to its contents.
The Company is committed to ensuring a high level of ethical and professional conduct and has zero tolerance for illegal or actions contrary to EU Law that could harm its reputation and reliability, through the combined application of the WPEUL and the Codes, Policies, and Procedures adopted by the Company.

1.2 Definitions

In accordance with the provisions of Article 3 of Law 4990/2022, the following definitions apply within the scope of the WPEUL and Law 4990/2022:

- Report: The oral or written provision of information regarding violations within the Company.
- Internal report: The oral or written or electronic platform-based provision of information regarding violations to the Company's Responsible Officer for Receiving and Monitoring Reports (RORMR).
- External report: The oral or written or electronic platform-based provision of information regarding violations to the National Transparency Authority (NTA).
- Inadmissible report: A report that refers to a violation but does not fall within the scope of Article 4 of Law 4990/2022 or is not clear, specific, complete, timely, or is evidently malicious, frivolous, or excessive.
- Whistleblower: The natural person who reports or discloses information regarding violations that they have obtained in the course of their employment or cooperation with the Company.
- External associates: Third parties who are contractually or otherwise connected with the Company, its personnel, as well as consultants, subcontractors, contractors, suppliers, collaborators of all kinds, shareholders, etc.
- Responsible Officer for Receiving and Monitoring Reports (RORMR): The Company official responsible for receiving, managing, and coordinating the investigation of reports by the Reporting Evaluation Committee. The RORMR is appointed by a decision of the Company's Board of Directors for a three-year term and may be replaced by a subsequent Board decision.
- Reporting Evaluation and Management Committee (REMC): The committee that manages reports, conducts preliminary investigations, and prepares the final investigation report for the Company's Board of Directors. It consists of the following members: 1) the RORMR, 2) the Data Protection Officer, 3) an administrative employee of the Company appointed by the Board of Directors with a three-year term.
- Employee: The natural person employed by the Company under a fixed-term or indefinite employment contract, or another employment relationship, or a person who is seasonal staff or an intern of the Company.
- Reasonable grounds: Grounds that justify the belief of a person, with similar knowledge, training, and experience to the whistleblower, that the information they possess is true and constitutes a violation of EU law and falls within the scope of this policy.
- Personal data: Personal data as defined in Regulation (EU) 2016/679 and Law 4624/2019.
- Retaliation: Any direct or indirect act or omission that takes place in the workplace as a result of the report and causes or may cause unjustified harm to the whistleblower, or place them at a disadvantage, and is related to an internal or external report or public disclosure. Retaliation may include, but is not limited to, harassment, any form of discriminatory treatment, negative performance evaluation, wage freeze or reduction, assignment of different or lesser duties, and generally any form of adverse change in employment terms.

2. Scope of Application

Under the framework of the current Whistleblower Policy on Violations of EU Law (WPEUL), individuals working for or providing services to the Company are encouraged to report serious irregularities, violations, or criminal acts that come to their attention and concern any person working for or providing services to the Company.

Specifically, the provisions of Article 6 of Law 4990/2022 apply to: a) Employees, regardless of whether their employment is full-time or part-time, permanent or seasonal, or if they are temporary workers. b) Non-salaried individuals, self-employed, consultants, or home-based workers. c) Shareholders and individuals who belong to the administrative, managerial, or supervisory bodies of the company, as well as volunteers and interns, whether paid or unpaid. d) Any individuals working under the supervision and direction of contractors, subcontractors, and suppliers of the Company. e) Individuals who report or publicly disclose information regarding violations acquired within the scope of an employment relationship that has ended for any reason, including retirement, as well as whistleblowers whose employment relationship has not yet begun in cases where information regarding violations was obtained during the recruitment process or another stage of negotiation prior to contract conclusion.

The protection measures for whistleblowers under Law 4990/2022 also apply, as appropriate, to: a) Intermediaries, b) Third parties connected to the whistleblowers who may suffer retaliation in a work-related context, such as colleagues or relatives of whistleblowers, and c) Personal businesses or legal entities in which the whistleblowers have an interest, or for which they work, or are otherwise connected through an employment relationship.

3. Subject of Reports

The Policy covers, indicatively, reports or complaints concerning:

- Violations of EU law, as specifically outlined in Part I of the Annex of Law 4990/2022, in the fields of:
  - Public procurement
  - Financial services, products, and markets, as well as the prevention of money laundering and terrorist financing
  - Product safety and compliance
  - Transport safety
  - Environmental protection
  - Personal data protection
  - Radiation protection and nuclear safety
  - Food and feed safety, as well as animal health and welfare
  - Public health
  - Consumer protection
- Violations that affect the financial interests of the EU under Article 325 of the Treaty on the Functioning of the European Union (TFEU) and as specifically defined in related EU measures.

- Violations of rules related to the internal market, as referred to in paragraph 2 of Article 26 of the TFEU, including violations of EU competition and state aid rules, as well as violations concerning the internal market regarding actions that breach corporate taxation rules or arrangements aimed at securing a tax advantage that undermines the purpose or objective of applicable corporate tax legislation.

It is clarified that:

- Violations concerning workplace violence and harassment are reported to the Responsible Officer for Receiving and Monitoring Reports (RORMR).
- Violations concerning personal data are reported to the Data Protection Officer.
- Violations concerning network security and the leakage of highly confidential (and classified) information are reported to the Head of the Technical Support Department (IT).

The management of these reports is handled in accordance with the specific policies and procedures adopted by the Company for the respective subjects.

4. Protection of Anonymity – Protection Against Retaliation

Reports are submitted when there is a sincere and reasonable belief by the whistleblower that a criminal act or offense has been or may have been committed concerning the issues mentioned above. In any case, the prerequisite is that there are reasonable grounds for the report, meaning a justified belief that the information is true and constitutes a violation of EU law.

Individuals who submit anonymous reports or publicly disclose violations but are later identified and face retaliation are entitled to the protection provided.

Whistleblowers are protected from any retaliatory actions or revenge. Specifically:

Confidentiality is ensured, and the whistleblower's identity is protected, as stipulated in the provisions of Article 10, paragraph 2(e), and Articles 13 and 14 of Law 4990/2022.

The submitted reports are disclosed only to predefined individuals who are deemed necessary to know in order to conduct an investigation, and they are bound by their duties to observe confidentiality and discretion. This also ensures the protection of the identities of the individuals involved in the report.

- Disclosure of the whistleblower's identity, if known, may be required during judicial or other legal proceedings as part of investigating the relevant case. In particular, the whistleblower is informed in writing before their identity is revealed unless such notification would undermine related investigations or legal processes. When informing the whistleblower, the Company provides explanations for the reasons behind the disclosure of such confidential information.

- Disclosure is made only if necessary for the purposes of Law 4990/2022 or to ensure the legal defense rights of the person against whom the report/complaint is made.
- The Company ensures that the whistleblower is adequately protected from negative consequences, such as threats or the application of retaliation, discrimination, or any form of adverse treatment. Any act of discrimination or retaliation, as referred to indicatively in Article 17 of Law 4990/2022, against a person who makes disclosures or may discourage others from making disclosures, is not tolerated.
- Protection covers both the individuals making the disclosures, provided they reasonably believe that the wrongful behaviors occurred or will occur, even if the allegations later prove inaccurate, and those who assisted or are connected with the whistleblowers.

The person or persons who are the subject of the disclosure are also entitled to protection and are covered by the presumption of innocence.

II. Procedures for Submitting Reports – EDAA

1. Submission of Reports

1.1. Reports can be submitted either in writing or orally, as follows:

a) A written report can be submitted:

(i) In person or by post to the company's headquarters at Farsalon 153, 41335, Larissa, in an envelope labeled "Attention: Responsible Officer for Receiving and Monitoring Reports (RORMP)" or "Report under Law 4990/2022" or with another indication that suggests the report falls under the provisions of Law 4990/2022, or

(ii) By email to the address: whistleblowing@prognosis-biotech.com.

b) An oral report can be submitted:

(i) By phone at +30 2410 623922. The content of the report submitted by phone is documented with a full and accurate transcription of the conversation into a record drafted by the RORMP, allowing the whistleblower to verify, correct, and agree with the final transcript by signing the relevant document.

(ii) Through a personal meeting with the RORMP, within a reasonable time from the date of the request. In this case, the RORMP keeps precise minutes of the meeting in a permanent and retrievable form, either by recording the conversation (with the whistleblower's legal consent) or in written form, which the whistleblower can verify, correct, and agree upon by signing them.

1.2. The ΥΠΠΑ assists the whistleblower in submitting their report by providing, upon request, any necessary information about their rights and the procedure for handling reports.

Anonymous reports can also be submitted. However, such reports make it extremely difficult or even impossible to conduct a thorough investigation of an incident, due to the challenge of obtaining information from an anonymous person (e.g., discussions for clarifications during the investigation) and due to the difficulty in assessing the credibility of the report. Anonymous reports are evaluated based on whether it is possible to identify and prove the illegal actions described without further information from the whistleblower.

1.3. In any case of a report, the following elements are necessary for the report to be considered specific and complete:

- Description of the wrongful behavior
- Identification of the time period of the incident
- Contact information at the discretion of the person making the disclosure, if they choose to reveal their identity
- Any document or information that contributes to the exposure/proof of the wrongful behavior.

2. MANAGEMENT OF PERSONAL DATA

Any processing of personal data within the framework of this policy is carried out in accordance with national and European legislation applicable to personal data, as well as the Company's personal data protection policy. The data of all involved parties are protected and processed solely in relation to the respective Report, with the sole purpose of verifying the validity of the Report and investigating the specific incident.

The Company takes all necessary technical and organizational measures to protect personal data, in accordance with its data protection policy as currently in force. Sensitive personal data and other data that are not directly related to the report are disregarded and deleted in accordance with the principle of data minimization.

Access to the data included in the reports is granted only to those involved in the management and investigation of the incident, such as members of the IIC (Internal Investigative Committee) and the UPPA (Whistleblower Protection Officer), including other specialized external advisors whose assistance may be requested by the IIC.

Personal data is deleted from the Report Registry within a reasonable time after the completion of the investigation initiated based on the Report. The Data Protection Officer (DPO) assists with the overall management of personal data.

3. MANAGEMENT OF SUBMITTED REPORTS

3.1. For the successful conduct of investigations, the Whistleblower Protection Officer (WPO) and the members of the Internal Investigative Committee (IIC) are granted:

- Unrestricted and unlimited access to all necessary company files and facilities related to the investigation.

- Authorization to examine and retrieve files or copies of them, in any form—physical or digital—as well as any kind of objects from any company facility, without prior consent or notification of the individual who may be using or storing the aforementioned, provided they fall within the scope of the investigation and after notifying and receiving approval from the company's administrator.

3.2. Both the UPPA and the other members of the EDAA are required to:

- Perform their duties with integrity, objectivity, impartiality, transparency, and social responsibility.
- Respect and maintain confidentiality and discretion regarding matters they become aware of during the performance of their duties.
- Refrain from managing specific cases by declaring a conflict of interest when such a conflict arises.

3.3. Once the UPPA receives a report, they initially check its validity and completeness regarding the required information and forward it to the other members of the EDAA for evaluation and further investigation. The EDAA decides on the appropriate actions on a case-by-case basis.

3.4. In the case of a verbal report, the minutes prepared by the UPPA, once signed by the whistleblower, serve as a receipt confirmation of the report. If the whistleblower refuses to sign the minutes, this is noted by the drafter.

3.5. If the report is received by an unauthorized person, they are obligated to immediately forward it to the UPPA of the Company, without altering its content or disclosing any information that could lead to the identification of the whistleblower or any third party mentioned in the report.

3.6. To avoid conflicts of interest, if a report involves a member of the EDAA, the UPPA is responsible for notifying the Company’s CEO, who will assign a replacement. If the UPPA themselves are involved, they are limited to registering the report in the special protocol book or relevant file and forwarding it to the National Transparency Authority as an external reporting channel, informing the whistleblower.

3.7. Acknowledgment of receipt of the report is sent to the whistleblower within seven (7) working days from receipt, regardless of the method of submission. The acknowledgment can be sent by any appropriate means, provided it can be proven and confidentiality and personal data protection requirements are always met. The UPPA is not required to send an acknowledgment if it is impossible to do so due to a lack of necessary contact information for the whistleblower.

3.8. The report, regardless of how it is submitted, is recorded in a special file maintained by the Whistleblower Protection Officer (UPPA) in either paper or digital form. The minimum retention period for these records is set at 5 years from the date the report is received, unless there are other legal reasons to extend the retention period (e.g., ongoing judicial investigation).

3.9. Upon receiving the report, the Internal Investigative Committee (EDAA) reviews and determines whether the submitted report concerns irregularities, omissions, or criminal acts. They then decide on the investigation actions that will lead to a final determination of whether the report is valid, accompanied by relevant documentation of the alleged violations. Anonymous reports are reviewed based on the ability to substantiate them and identify the irregular action reported. All reports are handled with care, impartial judgment, and objectivity, and at the end, a report with the findings and conclusions is prepared by the EDAA, which is forwarded to the Company's Board of Directors. It is clarified that, in the event of a lack of unanimity, each EDAA member has the right to record their opinion in the final report.

3.10. The EDAA may then proceed with one of the following actions: a) Transmit the report for investigation, anonymized and in accordance with confidentiality and personal data protection provisions, to:

aa) The appropriate company bodies, while documenting the action in the special protocol book or file maintained for this purpose.
ab) The appropriate authorities, while documenting the action in the special protocol book or file maintained for this purpose. Such authorities may include the Economic Crime Prosecutor, prosecutorial authorities in general, the National Transparency Authority, the Competition Commission, the Bank of Greece, the Data Protection Authority, the Hellenic Competition Commission, the Single Public Procurement Authority, the Hellenic Atomic Energy Commission, the Unified Food Control Authority, the Consumer Ombudsman, the National Cybersecurity Authority, the Anti-Money Laundering and Counter-Terrorism Financing Authority, the Independent Authority for Public Revenue, and the General Directorate for Financial Crime Enforcement.
b) File the report, with a decision communicated to the whistleblower (if feasible), under the following circumstances:

ba) The report is clearly unreasonable, vague, incomprehensible, or repeated in an abusive manner, such as in cases of resubmission of the same content without providing new information.
bb) The report’s content does not fall within the scope of Article 4 of Law 4990/2022. If, however, the report contains information regarding violations under the jurisdiction of another body within the organization or another public entity, the UPPA is required by Article 4 of the Administrative Procedure Code to forward it to the appropriate body. In this case, there is no longer an obligation to monitor the report under section 6 of paragraph 2, Article 10 of Law 4990/2022.
bc) There are no substantial indications of violations that fall within the scope of Article 4 of Law 4990/2022.

3.11. In the event that new evidence is provided for a report that has already been archived, the UPPA shall retrieve the archived report and proceed with the necessary actions to examine this new evidence.

3.12. If the UPPA discovers indications of a criminal act that is prosecutable ex officio from the provided evidence, they must promptly forward a copy of the report to the

competent Prosecutor, informing the whistleblower. If the violation falls within the scope of Law 4990/2022, the forwarding must be done in accordance with the confidentiality and personal data protection provisions, and the UPPA is also required to monitor the report as stipulated in item (f) of paragraph 2, Article 10 of the same law.

3.13. If the violation does not fall within the scope of Law 4990/2022, a copy of the report is forwarded to the appropriate authority without the obligation of further monitoring as specified in item (f) of paragraph 2, Article 10 of the aforementioned Law.

3.14. Based on the results of the investigation and if there are substantiated inappropriate behaviors and actions, the Company's Board of Directors, considering the recommendation of the EDAA, decides on corrective or disciplinary/legal actions. These actions may include (but are not limited to): a) further investigation if it deems the evidence insufficient for a complete resolution of the case, b) additional employee training, c) implementation of new internal control measures, d) amendments to existing policies and/or procedures, e) disciplinary actions including dismissal or termination of the reported individual, or f) reporting or other required actions to judicial or other competent authorities.

3.15. After completing the investigation, the UPPA informs the whistleblower (if the report was not anonymous) of the decision made regarding their report. A case is considered closed when a final decision has been made by the Company's management following their review of the EDAA's report. Feedback to the whistleblower is provided no later than three (3) months from the acknowledgment of receipt of the report or, if no acknowledgment was sent, three (3) months from the end of the seven-day period after the report submission.

3.16. However, if the whistleblower believes that their report was not effectively addressed, they may resubmit it to the **National Transparency Authority** (hereinafter "**NTA**"), which, as the External Reporting Channel, exercises its legally prescribed responsibilities according to Article 12 of Law 4990/2022. For additional information on submitting a complaint to the NTA, interested parties can refer to the Authority's website: https://aead.gr/submit-complaint.

3.17. Exceptionally, if a report is proven to be false and/or malicious, and if the accused requests it, they may be informed of the whistleblower's identity to exercise their legal rights. It is clarified that reports proven to be blatantly false and/or malicious will be further investigated at the discretion of the Company's Board of Directors, both regarding the motives and the individuals involved, in order to restore order using all legal means and methods.

3.18. Whistleblowers have access to all legal remedies and assistance, enjoy the rights to a fair trial, and in particular, the right to a fair hearing before an impartial court, as well as the presumption of innocence and defense rights, including the right to be heard and the right to access their file. The identity of individuals reported in the complaint is protected throughout the investigations initiated by the report or public disclosure.

III. APPROVAL, REVIEW, AND COMMUNICATION

The PPPD (Policy on the Protection of Personal Data) is approved by the Company's Board of Directors, which is also responsible for reviewing it whenever deemed appropriate.

Under the responsibility of the DPO (Data Protection Officer), the PPPD is communicated to the Staff and published on the Company's website in a separate, easily recognizable, and accessible section.

The DPO ensures that all Company employees are informed about the content of this Policy. The communication is carried out through appropriate means, such as sending printed informational materials, emails, newsletters, depending on the category of employees and their access possibilities.

The Board of Directors informs the DPO of any revisions or reissues of the PEPD so that the necessary actions can be taken to communicate the updated version.

For matters not covered by this Policy, the provisions of Law 4990/2022 and any other relevant regulatory provisions apply.

Edition	Date	Description	Approval
1η	15.12.2023	Initial Issuance of Policy and Procedures for Managing Reports Regarding Violations of EU Law	12.1.2024 Board of Directors Meeting