

Whistleblower protection policy

Company: "Maneuver LT" UAB

Approval/ Review: 2025-09-11 No.2025-V-33

Applicable laws:

[The Law on the Protection of Whistleblowers of the Republic of Lithuania](#)

[METHODOLOGICAL GUIDE FOR THE PRACTICAL APPLICATION AND IMPLEMENTATION OF THE LAW ON THE PROTECTION OF THE WHISTLEBLOWERS OF THE REPUBLIC OF LITHUANIA](#)

[Directive \(EU\) 2019/1937 of the European Parliament and of the Council.](#)

Responsible for the revision of the Policy: Legal and Compliance Unit

1. General part

1. The purpose of this Policy is to enable and encourage the Company's employees (current and former) and their Family members, clients, service providers, or other parties to contractual and pre-contractual relationships, members of management and supervisory bodies, and shareholders to Report actual or potential Breaches of laws, internal policies, and procedures without fear of negative consequences.
2. This Policy regulates the procedure for submitting, receiving, registering, evaluating, and making decisions regarding information about Breaches received through the Company's internal channel for Reporting Breaches (hereinafter, the **Reporting Channel**).

3. The following definitions and terms are used in this Policy:

Authorized Person - chief legal and compliance officer, who is a person appointed by the Company's decision, responsible for receiving, registering, and examining Reports, making a decision, and informing the Whistleblower and/or competent authorities.

Competent authority - Prosecutor's Office of the Republic of Lithuania.

Confidentiality - the Company's operating principle that ensures data of the person providing information about a Breach and other information that directly or indirectly identifies them is processed only for the purpose of performing work functions, and that this information is not disclosed to third parties.

Facilitator - a natural person who helps the person submitting information about a Breach and whose assistance should be confidential.

Breach - a criminal offense, administrative offense, disciplinary offense, or Breach of work duties that is potentially being prepared, committed, or has been committed within the Company, as well as a gross Breach of mandatory and/or declared business ethics norms, an attempt to conceal such a Breach, or any other legal Breach that poses a threat to or infringes upon the Company, stakeholders, or the public interest. The Whistleblower learns about these Breaches through their current or former employment, or contractual relationships (e.g., consultation, contracting, subcontracting, internship, practice, volunteer work) with the Company, or during employment or other pre-contractual relationships.

Whistleblower - a natural person who submits information about a Breach in an institution that they learned about through their current or former service, employment, or contractual relationships (e.g., consultation, contracting, subcontracting, internship, practice, volunteer work) with this institution, or during employment or other pre-contractual relationships. This also includes a person who has the status of a self-employed person, a shareholder, or a person belonging to the Company's administrative, management, or supervisory body (including non-executive members, as well as volunteers and paid or unpaid

interns), or any natural person working under the supervision and direction of contractors, subcontractors, and/or suppliers.

LPAW - the Law on the Protection of Whistleblowers.

Policy - this Whistleblower Protection Policy.

Report - a Report that contains specific information about a Breach.

Work-related circumstances - current or former work activities of any kind at the Company during which individuals learned about a Breach and could face negative consequences if they Reported it.

Person involved in the Breach - a natural or legal person identified in the Report as possibly preparing to commit, committing, or having committed a Breach, or a person associated with that Breach.

Family members - parents (adoptive parents), children (adopted children), siblings, and their spouses living with the person, as well as the person's spouse or a person with whom the person cohabits without registering a marriage (partnership), and the spouse's parents.

2. Submission of reports

1. Any Whistleblower can submit a Report through the internal Reporting channel.
2. The basis for submitting a Report is the information the person has about a Breach at the Company.
3. When submitting a Report, the Whistleblower is not required to be completely certain of the truthfulness of the Reported facts, and they are not obliged to assess whether the Breach they are Reporting meets the characteristics of a criminal offense or other legal Breaches as defined in

legal acts. However, the Reporting Channel may not be abused by knowingly providing false and/or unsubstantiated information about a Breach and/or for achieving unlawful and/or unethical personal goals.

- 4.** The Company expects the Whistleblower to Report any Breach or good-faith doubt about possible Breaches of the laws of the Republic of Lithuania and/or the Company's policies or other internal legal acts.
- 5.** Below is a non-exhaustive list of information that a Whistleblower should Report in accordance with the procedure set forth in this Policy:
 - 5.1.** danger to public safety or health, or to a person's life or health;
 - 5.2.** danger to the environment;
 - 5.3.** obstruction or unlawful influence on investigations conducted by law enforcement authorities or courts in the administration of justice;
 - 5.4.** financing of illegal activities;
 - 5.5.** unlawful or non-transparent use of public funds or assets;
 - 5.6.** property acquired by illegal means;
 - 5.7.** concealment of the consequences of a committed Breach, or obstruction of determining the extent of the consequences;
 - 5.8.** Breaches specified in the list approved by the Minister of Justice of the Republic of Lithuania, prepared in consideration of the scope of the European Union legal acts referred to in Directive (EU) 2019/1937;
 - 5.9.** harming the financial interests of the European Union, as specified in Article 325 of the Treaty on the Functioning of the European Union and described in more detail in related European Union measures;
 - 5.10.** Breaches related to the internal market, as specified in Article 26(2) of the Treaty on the Functioning of the European Union, including Breaches of

European Union competition and state aid rules, as well as internal market-related Breaches due to actions that Breach corporate tax rules, or agreements aimed at obtaining a tax advantage that undermines the subject or purpose of the applicable corporate tax law;

5.11. Breach of international sanctions implemented in the Republic of Lithuania or restrictive measures established by the laws of the Republic of Lithuania;

5.12. Breaches of the Company's internal legal acts;

5.13. other Breaches.

6. The Whistleblower can submit Reports through (**Reporting Channels**):

a) By email at **whistleblow@genome.eu**

b) In writing directly to the Authorized Person.

c) In writing directly to the Head of the Company or the chairman of the board, if the Report is related to a Breach allegedly committed by the Authorized Person. A Report submitted to any of the Company's board members' business email addresses is considered to be properly delivered to the Company's board. The board member who receives the Report must immediately inform all other Company board members.

The Authorized Person (or, in their absence, the person substituting for them) is the only one who has access to the data/information submitted through the Reporting Channels specified in clauses 4.6(a)-(b) of the Policy.

7. Any Company employee who receives a Report at their business email address must immediately forward the received Report to the Reporting Channel.
8. A Report is submitted:
 - a) Using the form provided in Annex No. 1 (by filling it out and submitting it through one of the Reporting Channels); or
 - b) As a free-form Report, which must:
 - b.1. state that the information is provided in accordance with this Policy and/or the Law on the Protection of Whistleblowers (not applicable when submitted through a channel specially dedicated to Reports, i.e., the channel specified in clause 3.4(a));
 - b.2. list the specific factual circumstances that led the Whistleblower to suspect a Breach;
 - b.3. indicate whether the Breach has been Reported to anyone else and whether a response has been received;
 - b.4. include any information known to the Whistleblower about the alleged Breacher(s) (name, surname, position);
 - b.5. include any information known to the Whistleblower about the witness(es) to the Breach (name, surname, position);
 - b.6. include any other information known to the Whistleblower about the Breach, data, documents, or information held by the Person involved in the Breach, or where such data or documents could be found;
 - b.7. express a desire to be informed about the receipt of the Report at the Company;
 - b.8. state the Whistleblower's name, surname, personal code, residential address, or email address for correspondence and other contact details.

The person can also specify how and when it is best to contact them. The Report can also be anonymous.

9. A person submitting information about a Breach can directly contact a competent authority with a Report about the Breach if at least one of the following circumstances exists:
 - 9.1. The Breach is of significant public interest;
 - 9.2. It is necessary to prevent or stop the Breach as soon as possible, as significant damage may occur;
 - 9.3. Persons in a management position or those connected to the institution by employment, service, or contractual relationships may themselves be committing or have committed Breaches;
 - 9.4. Information about the Breach was submitted through the internal Reporting channel, but no response was received, or no action was taken in response to the submitted information, or the measures taken were ineffective;
 - 9.5. There are grounds to believe that the anonymity or confidentiality of the person submitting information about the Breach may not be ensured, or that there will be an attempt to conceal the Reported Breach, or that the person submitting information about the Breach will face negative consequences;
 - 9.6. There is no functioning internal Reporting channel in the institution;
 - 9.7. The person submitting information about a Breach cannot use the internal Reporting channel because they are not connected to the institution by employment, service, or other legal relationships.

3. Receiving and examining reports of breaches

1. A Report received through the Reporting channel(s) is registered by the Authorized Person on the same business day in the internal Whistleblower Report Registration Log, except in cases specified in clause 4.6(c) of the Policy.
2. When the Whistleblower's contact details are provided in the Report, the Authorized Person informs the Whistleblower about the receipt of their Report at the Company no later than within 2 business days after receiving the Report and specifies the next steps and their deadlines.
3. The Whistleblower is not informed about the receipt of the Report when:
 - a) The Report was submitted anonymously;
 - b) The Whistleblower expressed a wish in the Report not to confirm the receipt of the Report and/or not to provide any other information about the examination of the Report;
 - c) Confirming the receipt of the Report would jeopardize the Whistleblower's confidentiality.
4. No later than within 10 business days of receiving the Report, the Authorized Person must examine the information provided in the Report and, except in cases specified in clause 5.3 of the Policy, inform the Whistleblower about the progress of the examination of the information

(planned or completed examination actions, their justification) or the refusal to examine this information.

5. If the Company receives a Report containing information that it is not competent to evaluate, it forwards the Report to the competent authority no later than within 2 business days from the date of receipt of the Report and, except in cases specified in clause 4.3 of the Policy, informs the Whistleblower about it.
6. The duration of the investigation must not exceed three months from the confirmation of the receipt of the Report, or, if confirmation was not sent to the Reporter, a period of three months from the end of the 2-business-day period after the Report was submitted.
7. The Authorized Person, after completing the investigation of the information provided in the Report, prepares a draft decision and proposed measures for preventing the Breach and/or holding the person who committed the Breach accountable and eliminating the consequences of the Breach, and submits it for approval to the Head of the Company or, when the Report was related to a Breach allegedly committed by the Head of the Company, to the Company's board. The Head of the Company or the board makes the final decision based on the material from the Authorized Person's investigation, the proposed decision, and the measures.
8. No later than within 2 business days from the adoption of the decision by the Head of the Company or board, the Authorized Person informs the Whistleblower about the adoption of the decision, its essence, and the measures to be applied, except in the cases specified in clause 5.3 of the Policy.
9. A Report is not examined, and the Whistleblower is informed about this, if:
 - a) The Report is based on information that is obviously untrue;

b) The Whistleblower reapproaches the Company regarding the same circumstances after a previously submitted Report was examined in accordance with the procedure established by the Policy and a decision was made on it, or the examination was refused.

- 10.** The Authorized Person informs the person who submitted the information about the Breach about the decision not to examine the Report and its reasons, no later than within 2 business days from the date of the decision, except in cases specified in clause 5.3 of the Policy.
- 11.** If new legal or factual circumstances arise that did not exist or were not known when the decision to refuse to examine the Report was made, the Authorized Person, the Head of the Company, and/or the board may decide to examine the Report.
- 12.** In cases where the Breach that the Whistleblower wishes to Report is being committed by and/or is related to the Authorized Person, the Whistleblower may submit the Report directly to the persons specified in clause 4.6(c) of the Policy (i.e., the Head of the Company or board). The Head of the Company or board, upon receiving the Report, immediately appoints a person who will be responsible for examining this Report, investigating the circumstances specified in it, and preparing a draft decision and submitting it to the Head/board for approval. Such a person appointed to examine the Report must perform all actions assigned to the Authorized Person's responsibility as specified in the Policy. The receipt of the Report and its subsequent stages of examination in this case are registered in the Report Registration Log immediately after the Head of the Company or the board adopts and approves a decision regarding the Breach specified in the Report.

4. Whistleblower protection measures

1. From the moment the Report is received, the Whistleblower's confidentiality is ensured to the extent that it is objectively possible, given the data provided and their connection to the Whistleblower.
2. Information about Whistleblowers, persons involved in the Breach, or Facilitators is not and cannot be provided to persons not participating in the Report/Breach investigation, except in cases specified in clauses 6.3-6.4 of the Policy.

Company employees, members of management, and/or supervisory bodies who, by their duties, have become aware of the Whistleblower's personal data or the information provided in the Report, must ensure the confidentiality of the information and personal data during their employment at the Company, as well as after moving to another position or after the termination of the employment relationship.

3. The data of the Whistleblower and/or the Person involved in the Breach, which allows their identity to be established, may be provided only to:
 - a) Those persons who are examining the information and making a decision about the Breach/Report;
 - b) When transferring information about the Report/Breach to an institution competent to examine it and/or in other cases provided for by law. Before providing confidential data to competent authorities/other persons in accordance with clause 6.3 of the Policy, the Authorized Person must notify the Whistleblower in writing about the provision of the data, stating the reason for providing the confidential data. The institution/person to whom such information is transferred ensures the confidentiality of the transferred confidential data in accordance with the procedure established by the LPAW.

4. Confidentiality is not ensured when:
 - a) The Whistleblower requests it in writing;
 - b) The Whistleblower provides knowingly false information.
5. This Policy prohibits all Company managers, members of management and/or supervisory bodies, shareholders, and employees from taking, threatening to take, and attempting to take negative measures from the moment a Report is submitted through the Reporting Channels. This includes, but is not limited to:
 - 5.1. temporary suspension from duties;
 - 5.2. dismissal from work;
 - 5.3. transfer to a lower position or another workplace, restriction of career opportunities;
 - 5.4. intimidation, coercion, harassment, discrimination, threats of reprisal;
 - 5.5. reduction of salary;
 - 5.6. questioning competence;
 - 5.7. negative evaluation of performance results or providing a negative reference about the employee;
 - 5.8. imposition or application of any disciplinary penalties or other sanctions (including financial sanctions);
 - 5.9. causing harm (including harm to a person's reputation, especially on social networks);
 - 5.10. applying any other negative measures.

6. It is prohibited to have a negative impact on the Whistleblower's Family members, relatives, or colleagues working at the Company or another legal entity subordinated to the Company, where the Whistleblower's family member, relative, or colleague may suffer negative consequences due to the submission of the Report.
7. These protection and defense measures for the Whistleblower, their Family members, relatives, and colleagues cannot be waived or restricted by agreements.
8. If the Whistleblower, their Family members, relatives, or colleagues have experienced a negative impact, the Company must prove in the event of a dispute that the negative consequences were not due to the submission of the Report.
9. When the Whistleblower, their Family members, relatives, or colleagues are experiencing a negative impact, they must Report it to the Authorized Person. If the negative impact is being caused by the Authorized Person, they must Report it to the Head of the Company and/or the Company's board, who must immediately take all reasonable measures to prevent such negative impacts and eliminate their negative consequences. A Breach of the prohibition on applying negative measures is considered a gross Breach of work or official duties, for which the most severe accountability measures may be applied, including the violator's dismissal from work/removal from office.

If the Authorized Person, the Head of the Company, or the board does not take measures to prevent negative consequences and/or eliminate the consequences caused by them, the Whistleblower has the right to apply directly to the competent authority, which decides on the recognition of the person as a Whistleblower in accordance with the LPAW. The competent authority, having recognized the person as a Whistleblower in accordance with the LPAW and having established that they are experiencing a negative impact, may set a deadline for the Company within which the consequences of the negative measures must be eliminated.

10. The Whistleblower, the Whistleblower's family member, relative, or colleague may apply to the court due to the consequences of the negative measures experienced.
11. At the request of the Whistleblower, the Authorized Person provides comprehensive, impartial information and free consultations on the procedures for submitting information about Breaches and the provision of remedies.
12. The Whistleblower does not incur any contractual or tort liability, or liability for insulting honor and dignity, or for defamation, if, when submitting information about a Breach in accordance with the procedure established by this law, they reasonably believed that they were providing correct information.
13. The Whistleblower is liable for damages resulting from the submission of the Report only if it is proven that the person could not have reasonably believed that the information they provided about the Breach was correct.
14. If the Report was anonymous, the Whistleblower protection measures specified in the Policy are applied in cases where their identity was disclosed and it is necessary to protect them from a negative impact.

5. Rights and duties of the authorised person

1. The Authorized Person, or another person appointed to examine a Report/Breach in accordance with this Policy, has the right to perform their assigned functions:
 - a) To obtain all information and data necessary for the investigation from Company employees and departments not subordinate to them;

b) To make decisions related to the investigation when examining a Report received through the Reporting Channel, which are binding on all employees and departments of the institution.

2. The Authorized Person:

a) Is responsible for the timely registration of Reports and each stage of the Report examination process in the Report Registration Log;

b) Consults the Company's management, members of management and supervisory bodies, shareholders, all other employees (current and former), their Family members and relatives, service providers or other parties to contractual and pre-contractual relationships, and any other persons working under the supervision of the Company's contractors, subcontractors, and suppliers, on matters of the possibility of submitting a Report, the examination of a Report, and the implementation of the rights granted to Whistleblowers under the Policy.

3. The Authorized Person, at least once a year:

a) Submits a Report/summarized data to the Company's board about the received and examined Reports, decisions made, and recommended changes to the Company's operations and processes to prevent Breaches from recurring and/or to ensure an effective Report examination process. The Report/summarized data is provided in a compliance Report.

b) Announces changes and/or updates to the Policy, if any have occurred, and familiarizes the Company's employees with it.

6. Final provisions

1. Information about the Authorized Person, their contacts, and the procedure for submitting and examining Reports at the Company is provided through the Company's internal communication channels—by having Company

employees, members of management and supervisory bodies, familiarize themselves with the Policy (with signatures).

2. The Authorized Person is responsible for the proper implementation, continuous supervision, and regular updating of this Policy. Changes to the Policy are approved by a decision of the Company's board.
3. The Company ensures the storage of information and records about Reports and Breaches, observing confidentiality requirements, for a period of no less than 5 years from the last decision made in the examination of this information.

7. Annexes

Annex No. 1. [Breach report form](#).