

WHISTLEBLOWING POLICY

I. GENERAL PROVISIONS

1. Whistleblowing policy (hereinafter referred to as the Policy) specifies the procedures for reporting breaches, protecting whistleblowers, and, where applicable, providing remuneration for information on breaches. It has been prepared in accordance with the requirements of European Union and Lithuanian legislation, such as Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons on the protection of persons who report on breaches of Union law, and the Law on the Protection of Whistleblowers of the Republic of Lithuania (hereinafter referred to as LPW) implementing it, as well as the Company's commitment to prevent criminal activity and breaches that pose a threat to public and Company interests.

2. The purpose of the Policy is to establish the Company's internal process that ensures the rights and obligations of whistleblowers, the legal basis and forms of their protection, and measures for their safeguarding, encouragement, and assistance. It aims to provide appropriate opportunities to report infringements of law that threaten or violate public and Company interests, ensure their prevention and disclosure, and hold responsible individuals accountable. The Policy also provides whistleblowers with the means to report infringements via the internal Infringement Reporting Channel, ensuring confidentiality and security.

3. The Policy specifies procedures to ensure that reports are examined objectively and without delay, and that whistleblowers are protected from any adverse consequences.

4. Information on infringements is provided with the aim of protecting public and Company interests. The Policy does not apply where information is provided solely to defend personal interests (i.e., to protect the individual rather than the Company or public interest).

5. The Policy applies to all whistleblowers specified herein. The Policy and its Annexes, together with the link to the Channel through which reports may be submitted, are published:

5.1. On the Company's intranet (accessible to employees);

5.2. On the Company's website www.paysera.lt (publicly available to all whistleblowers).

6. For whistleblowers located outside the Republic of Lithuania, in addition to this Policy, the relevant local laws governing whistleblower protection shall also apply.

7. The definitions and terms used in this Policy are as follows:

7.1. **Responsible person** – an employee of the Company's Internal Audit Department, appointed by the order to administer the Channel, receive reports, conduct or coordinate investigations (if the investigation involves multiple persons), and ensure the Confidentiality of the Whistleblower. The Responsible person also includes a

deputy appointed by order to act in their place during periods of absence (e.g., business trips, illness, or vacations).

7.2. **Company** – Paysera LT, UAB, and its divisions where an Infringement may be committed, prepared, or occurring.

7.3. **Information on infringement(s)** – information provided by the Whistleblower via the Channel or directly/publicly to the Competent authority concerning an Infringement or infringements as defined in clause 13 of this Policy.

7.4. **Channel** – the internal Infringement Reporting Channel; the procedure applied by the Company for reporting infringements, conducting investigations, and informing relevant persons, including the technical and organisational measures established for this purpose.

7.5. **Competent authority** – a state or municipal institution legally empowered to perform whistleblowers protection functions under the LPW, conduct investigations, and receive information. In the Republic of Lithuania, such authorities include the Office of the Chief Official Ethics Commission, the Prosecutor’s Office, and other institutions authorised by law. In other jurisdictions, this refers to the relevant local competent authorities under national law.

7.6. **Confidentiality** – the principle governing the conduct of the Company’s employees, ensuring that the whistleblower’s data and any information that could directly or indirectly identify them are processed solely for the performance of work or official duties, and are not disclosed to third parties (including other employees) except as required by law. Information about whistleblowers must not be disclosed to persons not involved in the investigation. It is also ensured that information will not be revealed without the whistleblower’s consent, except where necessary to investigate an Infringement or as required by law.

7.7. **Assistant** – any natural person who assists the Whistleblower in the process of submitting a report and whose assistance is to be kept confidential.

7.8. **Infringement** – in the Company may be committed, prepared, or occurring:

7.8.1. A criminal offence;

7.8.2. An administrative offence, official misconduct, or violation of work duties;

7.8.3. A breach of professional ethics standards;

7.8.4. A violation of requirements established by the Company’s legal acts;

7.8.5. A breach of international sanctions;

7.8.6. A legal Infringement that poses a threat to or violates the public interest, of which the Whistleblower becomes aware through their existing or expected relationship with the Company.

7.9. **Policy** – the Policy on Reporting of Infringements, Whistleblower Protection, and Remuneration for Information on Infringements (Whistleblowing policy).

7.10. **Whistleblower (or person providing information on an infringement)** – a natural person who provides information to the Company about an Infringement of which they have become aware:

7.10.1. While having or having had an employment relationship with the Company;

7.10.2. During contractual relationships (including consulting, contract, subcontract, internship, practical training, voluntary work, or similar relationships);

7.10.3. During recruitment or other pre-contractual relationships;

7.10.4. While acting as a freelancer;

7.10.5. As a shareholder or a member of the Company's administrative, management, or supervisory body (including non-executive members, as well as volunteers and paid or unpaid interns);

7.10.6. On any other basis that entitles them to act on behalf of the Company.

7.11. **Report** – a communication submitted in writing, verbally, or electronically to the Responsible person, containing specific Information on an infringement that meets the characteristics specified in the Policy, and/or a communication to the Competent authority providing specific Information on an infringement that meets the characteristics specified in the Policy.

7.12. **Monitoring department** – the Company's Risk Management and Compliance Department, responsible for the independent monitoring and oversight of the implementation of this Policy.

II. RESPONSIBLE PERSON (INTERNAL AUDIT DEPARTMENT)

8. The Company has appointed a Responsible person and, during any period of their absence, a Deputy. Their appointment is formalised by an order of the Company's management, which applies together with this Policy.

9. Employees appointed as the Responsible person and the Deputy must have a reputation and qualifications that leave no doubt as to their ability to properly implement the provisions of this Policy.

10. No influence or other interference may be exerted on the Responsible person implementing the Policy, and they must be allowed to perform the functions assigned to them under this Policy. Disciplinary measures apply in the event of obstruction of the Responsible person in carrying out their functions.

11. Within the scope of their competence, the Responsible person performs the following functions:

11.1. Ensures that the Channel operates continuously and is easily accessible to all whistleblowers, including periodic updates of information on the Company's intranet, website, and other communication channels.

11.2. Receives Reports via the Channel, decides whether a separate investigation team is required, and, if necessary, initiates the issuing of an order to form such a team. Ensures that the members of the investigation team are trained to handle confidential information and comply with Whistleblower protection principles.

11.3. Analyses the Information on infringements received, investigates it, or organises and coordinates the investigation, ensuring objectivity, impartiality, and timely response.

11.4. Ensures the confidentiality of the Whistleblower and protection from any adverse consequences related to the submission of the Report.

11.5. Cooperates with whistleblowers and Competent authorities, providing and/or receiving necessary information.

11.6. Collects and maintains anonymised statistical data on the number of Reports received and their outcomes, and prepares and submits an annual report to the Company's management body no later than 31 March each year.

11.7. Ensures that Information on infringements submitted via the Company's Channel is stored in durable and, where necessary, recoverable media, in accordance with the Company's internal approved procedures. Once the investigation is completed and a final decision is made, all data in the register that is not required for further legal proceedings is anonymised, removing any direct links to the Whistleblower's identity.

11.8. Performs other functions specified in this Policy and in the LPW, necessary for the effective handling of Reports and ensuring the protection of whistleblowers.

12. In carrying out the functions assigned to them, the Responsible person has the right to:

12.1. Receive the information and data required from Company employees and divisions not subordinate to them, and to require their full cooperation, ensuring Confidentiality. Refusal to cooperate with the Responsible person shall be considered a basis for disciplinary action.

12.2. When investigating Information on infringements received via the Channel, make decisions related to the conduct of the investigation, which are binding on all Company employees and divisions.

12.3. Document Information on infringements provided verbally (during a face-to-face meeting) by preparing an accurate record of the conversation. In such cases, the Whistleblower is given the opportunity to review and correct the record and to express their consent by signing it.

III. SUBMISSION OF REPORTS

13. The Company ensures that every Whistleblower has the opportunity to report an Infringement via the Channel (as specified in clause 7.5 of the Policy) and encourages this before approaching a Competent authority, if the Infringement can be effectively remedied internally within the Company and if the Whistleblower believes there is no risk of retaliation. However, it is emphasised that the Whistleblower has the right to approach a Competent authority directly if there are reasonable concerns regarding potential adverse consequences or ineffective internal handling of the Report, as provided under the LPW.

14. A Whistleblower may submit Information on infringements:

14.1. Via the Company's Channel;

14.2. Directly to a Competent authority;

14.3. Publicly (in compliance with the conditions specified in the LPW).

15. The basis for providing Information on infringements is the Whistleblower's existing knowledge or reasonable suspicions regarding a possible Infringement within the Company.

16. Information on infringements is provided in relation to the following areas:

16.1. Threats to public safety or health, or to an individual's life or health;

16.2. Threats to the environment;

16.3. Obstruction of, or unlawful influence on, investigations conducted by law enforcement authorities or on courts administering justice;

16.4. Violations related to the prevention of illegal activities, money laundering, or terrorist financing;

16.5. Unlawful or non-transparent use of public funds or assets;

16.6. Illegally obtained assets;

16.7. Concealment of the consequences of an Infringement or obstruction of determining the extent of such consequences;

16.8. Infringements listed in the register approved by the Minister of Justice of the Republic of Lithuania, prepared in accordance with the scope of European Union law as specified in Directive (EU) 2019/1937;

16.9. Harm to the financial interests of the European Union, as referred to in Article 325 of the Treaty on the Functioning of the European Union and further described in relevant European Union instruments;

16.10. Infringements related to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including violations of European Union competition and state aid rules, as well as internal market-related infringements involving actions that violate corporate tax rules;

16.11. Violations of international sanctions implemented in the Republic of Lithuania or restrictive measures provided for under the laws of the Republic of Lithuania;

16.12. Other infringements affecting the public interest or posing a threat to the Company's interests.

17. Deadlines for the handling of Reports (mandatory LPW requirements):

17.1. The Company shall, no later than 2 working days from the date of receipt of Information on infringements, acknowledge receipt of the Report to the Whistleblower by email or by another method specified in the Report.

17.2. The Responsible person shall, no later than 5 working days from the date of receipt of the information, decide whether the information will be examined and inform the Whistleblower accordingly. If a decision is made not to examine the Report, the reasons must be provided in writing.

17.3. The Responsible person shall, no later than 3 months from the date of receipt of the Report, inform the Whistleblower of the results of the investigation and any actions taken. If the investigation cannot be completed within this period for objective reasons, the Whistleblower shall be informed, provided with an explanation, and given an anticipated date for the completion of the investigation.

17.4. These deadlines are mandatory and are intended to ensure timely and effective handling of Reports, as well as to maintain Whistleblower confidence and compliance with the requirements of the LPW.

18. A Whistleblower submitting Information on infringements via the Channel is not required to be fully certain of the accuracy of the facts reported. They are under no obligation to assess whether the Infringement reported constitutes a criminal offence or other violation of the law, as defined in legislation and/or the Company's internal regulations. It is sufficient to have reasonable grounds to believe that an Infringement may have occurred.

19. The Company guarantees Confidentiality to the Whistleblower in all cases of Reports of Information on infringements, regardless of the outcome of the investigation or whether the reported facts are confirmed. However, Confidentiality is not guaranteed if the Whistleblower knew that the information provided was false, i.e., deliberately submitted false information. Confidentiality may also not be ensured if the Whistleblower requests in writing that their identity be disclosed. A Whistleblower who knowingly provides false information is liable in accordance with applicable law. Protection and Confidentiality do not apply if the person submitting Information on infringements discloses state or official secrets.

20. The mere fact that the information provided is inaccurate (for example, the Whistleblower was unaware of circumstances relating to lawful Company activities that appeared unlawful to them) shall not be considered false information, and the Whistleblower shall not be deemed to have knowingly provided false information.

21. A Report of an Infringement may be submitted by the following methods:

21.1. In person to the Responsible person (an employee of the Internal Audit Department);

21.2. By registered mail to the Company's address: Pilaitės pr. 16, Vilnius, LT-04328, Lithuania, marked "Confidential. To the Internal Audit Department";

21.3. By email to reportingchannel@paysera.com (accessible only to the Responsible person);

21.4. Phone contact is not provided, in order to ensure maximum security and proper documentation.

22. When using the Channel, a Whistleblower submits Information on infringements by completing a Report of an Infringement in the prescribed form (Annexe No. 1 to the Policy) or by a free-form Report, which must contain the information specified in clause 24 of the Policy.

23. When providing Information on infringements verbally (directly to the Responsible person), it is the responsibility of the Responsible person to record all information required under clause 24 of the Policy, and it is the responsibility of the Whistleblower to ensure that the Information on Infringements is accepted and recorded to the full extent desired, but no less than that specified in clause 24 of the Policy. The personal data requested in the Report form is necessary for identifying the Whistleblower for purposes of granting protection and/or remuneration for Information on infringements. This data is retained for no less than five years from the date of receipt.

24. When submitting a Report, a Whistleblower provides:

24.1. Who committed, is committing, or intends to commit an Infringement, when, how, and what Infringement;

24.2. The date and circumstances of becoming aware of the Infringement;

24.3. Their name, surname, workplace, and other contact details (the Whistleblower may choose not to provide these, but this may complicate the investigation process and the provision of feedback);

24.4. if available, any documents, data, or information revealing indications of a possible Infringement.

25. Upon receiving Information on infringements via the Responsible person, the Company shall:

25.1. Assess whether the Information on Infringements complies with the provisions of the Policy and the LPW;

25.2. Verify whether the Information on infringements is sufficient to initiate an investigation;

25.3. Register the Report in a specially designated electronic system or electronic register, ensuring Confidentiality and the security of all related data, accessible only to authorised persons;

25.4. If it is determined that the Company is not competent to evaluate this Information, forward it to the Competent authority no later than 2 working days from the date of receipt of the Information on infringements and notify the Whistleblower accordingly.

IV. CONTACTING COMPETENT AUTHORITIES

26. A Whistleblower who has submitted Information on infringements, in relation to possible or actual adverse consequences connected with the submission of information, may consult a Competent authority regarding ways or means to protect their rights. In addition, pursuant to Article 11(3) of the LPW, a Whistleblower may contact a Competent authority regarding the Whistleblower status granted to them (as defined in Article 2(8) of the LPW).

27. A Whistleblower may directly contact a Competent authority regarding an Infringement when at least one of the following circumstances exists:

27.1. The Infringement is of material significance to the public interest;

27.2. It is necessary to prevent or stop the Infringement as soon as possible, as it may cause substantial harm;

- 27.3. Senior or other persons connected to the Company through employment, service, or contractual relationships may themselves be committing or have committed infringements;
- 27.4. Information on the infringement was submitted via the Channel, but no response was received, or no action was taken in response to the information, or the measures taken were ineffective;
- 27.5. There are grounds to believe that, if information is submitted via the Channel, the Whistleblower's anonymity or Confidentiality may not be ensured, the reported Infringement may be concealed, or the Whistleblower may be subject to adverse consequences;
- 27.6. There is no functioning Channel within the institution;
- 27.7. The Whistleblower cannot use the Channel because they have no employment, service, or other legal relationship with the Company;
- 27.8. They become aware of indications of criminal offences being planned, committed, or already committed.
28. If a Whistleblower has not received a response, or no action has been taken within the Company in response to the submitted Information, or the measures taken are insufficient to prevent the Infringement, they, pursuant to Article 4(3)(4) of the LPW, have the right to directly approach a Competent Authority and submit a Report in the prescribed form (Annexe No. 1 to the Policy).
29. A Whistleblower submits a Report to a Competent authority using the form approved by that authority or a free-form Report, indicating that the Report is submitted in accordance with national legislation implementing Directive (EU) 2019/1937 (in Lithuania – the LPW).
30. When submitting Information on infringements or a Report, the Whistleblower provides:
- 30.1. The specific factual circumstances of the Infringement;
- 30.2. The person who is planning to, is, or has participated in committing the Infringement;
- 30.3. Whether they have already reported this Infringement; if so – to whom and whether a response was received;
- 30.4. Their name, surname, personal identification number or date of birth (if no identification number is available), and contact details.
31. Where possible, the Whistleblower should attach written or other available evidence concerning the Infringement to the information submitted.
32. Reports submitted to a Competent authority are examined in accordance with the established procedure (in Lithuania – the LPW).
33. Information on infringements may be submitted publicly when:
- 33.1. The Whistleblower first submitted a Report via the Channel and/or to a Competent authority, but no appropriate action was taken within the period specified in the Policy;
- 33.2. The Whistleblower has reasonable grounds to believe that the Infringement poses a threat to human life, public health, or the environment, and urgent action is required to prevent such a threat.
34. To obtain statutory guarantees, a Whistleblower submitting information publicly must first apply to a Competent authority with a request.
35. A Whistleblower submitting information publicly is not subject to the provisions of Article 3(3) of the LPW, nor to the measure referred to in Article 8(1)(2) of the LPW.

V. STORAGE OF INFORMATION ON INFRINGEMENTS AND ENSURING CONFIDENTIALITY

36. The Company ensures the Confidentiality of the content of information received via the Channel and other data that may identify the Whistleblower by implementing the following measures:

36.1. The Responsible person does not disclose to anyone through which Channel, in what quality or scope Information on infringements was received. Other Company employees who become aware of such information in the course of their duties (e.g., IT personnel administering the email reportingchannel@paysera.com) maintain its confidentiality in the same manner as other confidential Company information.

36.2. The Responsible person ensures that Information on infringements received and related data (information, documents) are stored securely and may only be accessed by persons authorised to handle Information on infringements (e.g., employees assigned to conduct a specific investigation or commission members).

36.3. The Responsible person, to the extent possible, anonymises data, separates it, and stores any data that could identify the Whistleblower separately from the investigation materials.

36.4. Investigation materials concerning Information on infringements are marked with the Confidentiality label "Confidential" along with other information classification and distribution restriction markings established within the Company. Confidentiality of investigation materials is ensured regardless of the results of the investigation into the Information on infringements.

36.5. Upon completion of the investigation, all materials are retained for no less than five years, as provided in Article 7(1) of the LPW, and no more than ten years, unless otherwise directed by a Competent authority. Materials are destroyed in accordance with Company-approved internal procedures. The destruction of materials does not constitute declassification unless the Whistleblower has explicitly waived Confidentiality in writing or the information has lawfully become public.

36.6. To ensure the Whistleblower's Confidentiality, archived investigation materials are stored so that no unauthorised person can access them, except for the persons who conducted the investigation. Documents are archived in accordance with Company-approved internal rules.

36.7. The submission of a Whistleblower's data and other Information to pre-trial investigations or other Competent authorities investigating infringements, without disclosure to other parties, is not considered a breach of Confidentiality. If the Whistleblower so requests, the Responsible person informs the Whistleblower of the fact that such Information has been submitted to the Competent authorities.

37. Upon obtaining the Whistleblower's consent, the Company may record the receipt of Information on infringements using one of the following methods:

37.1. Preserving a recording of the conversation on durable media from which the relevant information can be retrieved;

37.2. Processing the information using a precise meeting record form prepared by the Responsible person.

VI. PROHIBITION OF ADVERSE ACTION

38. From the date of submission of information, no adverse action may be taken against a Whistleblower, nor may any threats or attempts to take such action be made, including, but not limited to:

38.1. Temporarily suspending them from their duties;

- 38.2. Dismissing them from employment or service;
 - 38.3. Halting a promotion to a higher position;
 - 38.4. Transferring them to a lower position or another workplace;
 - 38.5. Refusing to convert a fixed-term employment contract into a permanent contract when the employee has a legitimate expectation of being offered permanent employment;
 - 38.6. Failing to extend a fixed-term contract or terminating a fixed-term contract prematurely;
 - 38.7. Intimidation;
 - 38.8. Use of force;
 - 38.9. Harassment;
 - 38.10. Restricting participation in previously customary formal or informal activities, or excluding from such activities;
 - 38.11. Discrimination;
 - 38.12. Threats of retaliation;
 - 38.13. Limiting career opportunities or suspending training;
 - 38.14. Reducing salary;
 - 38.15. Unjustified changes to working hours or assigning additional tasks without justification, or delegating them to others;
 - 38.16. Casting doubt on competence;
 - 38.17. Negatively assessing performance or providing adverse feedback about the employee;
 - 38.18. Communicating negative information about the employee to third parties that could hinder future employment in the sector or industry;
 - 38.19. Removing the right to work with state or official secret information;
 - 38.20. Imposing or applying any disciplinary measures or other sanctions (including financial);
 - 38.21. Causing harm (including damage to reputation, particularly on social media);
 - 38.22. Causing financial losses (including business or income loss);
 - 38.23. Terminating supply or service contracts prematurely;
 - 38.24. Revoking licences or permits;
 - 38.25. Sending to psychiatrists or other medical specialists;
 - 38.26. Applying any other adverse measures.
39. The prohibition on adverse action against a Whistleblower applies to the employer and other Company employees.
40. It is also prohibited to take adverse action against:

- 40.1. Family members or relatives of the person providing Information on infringements;
 - 40.2. Colleagues working in the Company or in another legal entity subordinated to the Company, where they could suffer adverse consequences as a result of the submission of Information on infringements;
 - 40.3. Helpers assisting in the submission of Information on infringements in work-related circumstances;
 - 40.4. Legal entities that are owned by the person submitting Information on infringements, or for which the person works, or with which they are otherwise connected in work-related circumstances.
41. If a Whistleblower believes they are being subjected to adverse action as a result of submitting a Report, the Company must prove that the actions were motivated by objective reasons unrelated to the Report.
 42. If a Whistleblower believes they are being subjected to adverse action, they may:
 - 42.1. Contact the Responsible person (if the adverse action is not taken by the Responsible person);
 - 42.2. Contact the Company's management or Board;
 - 42.3. Contact a Competent Authority;
 - 42.4. Make use of other remedies provided under applicable law.

VII. REMUNERATION OF WHISTLEBLOWERS FOR VALUABLE INFORMATION

43. By decision of the Company's management, a Whistleblower may be awarded remuneration for valuable Information on infringements submitted to the Responsible person (i.e., the Company).
44. In this Policy, remuneration is understood as a one-time monetary payment for valuable Information on infringements submitted to the Responsible person (i.e., the Company).
45. Remuneration may only be awarded to a Whistleblower if all the following conditions are met:
 - 45.1. The Information on infringements provided by the Whistleblower is considered valuable when it has helped to prevent potentially significant financial loss, or has enabled the prevention, cessation, or investigation of a criminal offence.
 - 45.2. The remuneration awarded to a Whistleblower by decision of the Company is an independent decision of the Company and is not dependent on any decision of a Competent authority regarding remuneration granted on behalf of the state.
 - 45.3. The payment of remuneration must not compromise the Whistleblower's Confidentiality or reveal that the payment is for a Report of an Infringement, or that the recipient is a Whistleblower, unless the Whistleblower has waived Confidentiality in writing.
46. The amount of remuneration is determined by the Company's management, taking into account the following factors:
 - 46.1. The value of the Information and its impact on the Company;
 - 46.2. The extent of the harm avoided;
 - 46.3. The Whistleblower's level of cooperation during the investigation;
 - 46.4. Other significant circumstances.

47. Remuneration is paid confidentially to protect the Whistleblower's identity.

VIII. PREVENTIVE MEASURES, TRAINING AND MONITORING

48. Company obligations and principles of prevention:p>

48.1. The Company adheres to a zero-tolerance policy for any forms of retaliation or adverse action against Whistleblowers.

48.2. Company management at all levels is personally responsible for creating a safe and trust-based environment. They are expected to lead by example, encourage open discussions, and respond promptly to the first signs of inappropriate behaviour.

49. The Company organises mandatory training on the Whistleblower protection system, recognition of Infringements, and the operation of the internal Channel:

49.1. Training is conducted periodically, at least once every two (2) calendar years.

49.2. Newly recruited employees are provided the opportunity to familiarise themselves with the Policy and training materials no later than one (1) month from the commencement of their employment.

49.3. Participation in training is recorded in the Company's internal systems.

50. Independent monitoring and oversight of the implementation of this Policy is carried out by the Monitoring Department, ensuring supervision of the Report administration process conducted by the Responsible Person and evaluating whether the Responsible Person adheres to the established timelines, ensures data Confidentiality, and whether the measures for Whistleblower protection are effective.

IX. FINAL PROVISIONS

51. Pranešėjas už žalą, atsiradusią dėl Informacijos pateikimo, atsako tik tuo atveju, kai įrodoma, kad jis negalėjo pagrįstai manyti, jog teikiama Informacija apie pažeidimą yra teisinga, t. y. veikė tyčia, pateikdamas melagingą informaciją. A Whistleblower is only liable for any harm arising from the submission of information if it can be demonstrated that they could not reasonably have believed the Information on infringements to be correct, i.e., they acted intentionally by providing false information.

52. Other protection, incentive, and assistance measures not specified in this Policy are provided for in the LPW and other legislation establishing Whistleblower protection.

53. The Legal Department reviews the Policy at least once every two years and, where necessary, initiates amendments, taking into account changes in the legislation of the Republic of Lithuania and the European Union, practical experience in applying the Policy within the Company, and best practices among participants in the financial market.

54. This Policy comes into effect on the date of its approval. The Policy, its annexes, and information on the Reporting Channels are continuously published on the Company's intranet and are publicly available on the Company's website at www.paysera.lt.