Updated on: 2026-10-21

WHISTLEBLOWING POLICY

I. GENERAL PROVISIONS

1. The Policy on Reporting of Infringements, Whistleblower Protection, and Remuneration for Information on Infringements (the Whistleblowing Policy; hereinafter – the Policy) has been prepared in implementation of the requirements of legal acts of the European Union and of the Republic of Lithuania, such as Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law and the Law on the Protection of Whistleblowers of the Republic of Lithuania implementing it (hereinafter – the LPW), and of the Company's aim to prevent criminal acts and infringements which pose a threat to the public interest and to the interests of the Company.
2. The purpose of the Policy is to establish the Company's internal process which ensures the rights and duties of Whistleblowers, the grounds and forms of their legal protection, as well as the measures for the protection of, the encouragement of and the assistance to such persons, with a view to creating proper opportunities to report legal infringements which pose a threat to, or infringe, the public interest and the interests of the Company, to ensuring the prevention and disclosure of such infringements and the holding liable of the persons who have committed them. It is also to provide the Whistleblower with the opportunity to report an Infringement through the internal Infringement Reporting Channel, ensuring the Whistleblower's Confidentiality and security.
3. The Policy describes the procedures which ensure that Reports are examined objectively and without delay and that Whistleblowers are protected against any adverse consequences.
4. Information on infringements is submitted with the aim of protecting the public interest and the interest of the Company. The Policy does not apply to cases where Information on infringements is submitted with the aim of defending exclusively one's own personal interests (i.e. with the aim of defending the person and not the interest of the Company or the public interest).
5. The Policy applies to all Whistleblowers specified in this Policy. The Policy and its annexes, together with the link to the Channel through which Reports of Infringements may be submitted, are published:
    1. on the Company's intranet (access for employees);
    2. on the Company's website www.paysera.lt (publicly accessible to all Whistleblowers).
6. Whistleblowers located outside the Republic of Lithuania are, in addition to this Policy, also subject to the relevant local legal provisions governing the protection of Whistleblowers.
7. The definitions and terms used in this Policy:
    1. **Responsible person** – a person appointed by an order of the Company's manager (Chief Executive Officer), performing the function of the internal audit unit or of the risk and compliance management unit, authorised to administer the Channel, to receive Reports, to conduct an investigation or to coordinate it (where the investigation is carried out by several persons) and to ensure the Confidentiality of the Whistleblower.
    2. **Company** – Paysera LT, UAB and its units in which an Infringement may be being prepared, may

have been committed or may be being committed.

3. **Information on infringement(s)** – information about an Infringement or Infringements laid down in point 7.8 and/or point 16 of this Policy which is submitted by the Whistleblower through the Channel or directly or publicly to a Competent authority.
4. **Channel** – the internal Infringement Reporting Channel – the procedure applied in the Company for the submission of Information on infringements, its investigation and the informing of the person, and the technical and organisational measures intended for that purpose.
5. **Competent authority** – a State or municipal institution which is authorised by legal acts to perform the Whistleblower protection functions provided for in the LPW, to conduct investigations and to provide information. In the Republic of Lithuania, the functions of the competent authority laid down in the LPW are performed by the Prosecutor's Office of the Republic of Lithuania (paragraph 2 of Article 5 of the LPW). In other jurisdictions – the local competent authorities under national law.
6. **Confidentiality** – a principle of the Company's activities under which the Whistleblower's data and other information allowing the Whistleblower to be identified directly or indirectly are processed solely for the purposes of the administration and examination of Reports, the protection of the Whistleblower and the performance of other obligations laid down by legal acts. Access to such information is granted only to authorised persons and only to the extent necessary for the performance of their functions. Such information is disclosed to other persons only on the grounds laid down by legal acts and to the extent necessary. The need to investigate an Infringement does not in itself confer the right to disclose the identity of the Whistleblower. The obligation of Confidentiality continues after the completion of the investigation and after the expiry of the powers of the persons who processed the information.
7. **Assistant** – any natural person who assists the Whistleblower in the process of submitting the Report and whose assistance should be confidential.
8. **Infringement** – the following, possibly being prepared, being committed or committed in the Company:
    1. a criminal act;
    2. an administrative offence, official misconduct or a breach of work duties;
    3. a breach of professional ethics;
    4. a breach of the requirements laid down by the Company's legal acts;
    5. a breach of international sanctions;
    6. a legal infringement which poses a threat to, or infringes, the public interest and of which the Whistleblower becomes aware from their existing or former relations with this Company.
9. **Policy** – the Policy on Reporting of Infringements, Whistleblower Protection, and Remuneration for Information on Infringements (the Whistleblowing Policy).
10. **Whistleblower (or the person submitting Information on an infringement)** – a natural person who submits to the Company Information on an infringement of which they became aware:
    1. while having or having had employment relations with the Company;
    2. during contractual relations (including consultancy, contracting, subcontracting, traineeship, internship, voluntary activity and other similar relations);
    3. during recruitment or other pre-contractual relations;
    4. while acting as a self-employed person;
    5. while being a shareholder or a member of the administrative, management or supervisory body of the Company (including non-executive members, as well as volunteers and paid or unpaid trainees);
    6. while having, on any other basis, the right to act on behalf of the Company.

    In this Policy, the term "Whistleblower" is used in a broad sense and does not in itself mean that the person has been granted whistleblower status under the LPW. The Confidentiality applied by the Company and the prohibition of adverse action in respect of a Report based on a reasonable

belief do not depend on whether such status under the LPW has been granted.

11. **Report** – an application to the Responsible person submitted in writing, orally or by electronic means in the prescribed form, setting out specific Information on an infringement which meets the characteristics laid down in the Policy, and/or an application to a Competent authority by which specific Information on an infringement meeting the characteristics laid down in the Policy is submitted.
12. **Monitoring Unit** – the Company's risk and compliance management unit, responsible for the independent monitoring and control of the implementation of this Policy.

II. RESPONSIBLE PERSON

8. A Responsible person is appointed in the Company. Their appointment is formalised by an order of the Company's manager (Chief Executive Officer), which specifies the particular person administering the Channel; the order applies together with this Policy. Where the internal audit function is not separated out in the Company's organisational structure or has been transferred to an external service provider, an employee performing the risk and compliance management function is appointed as the Responsible person. A person to whose actions a Report relates or who has any other conflict of interest withdraws from its examination; where the Responsible person withdraws, the person examining the Report is appointed by the Company's manager. Where a Report relates to the Company's manager, the Responsible person registers the Report and forwards it without delay to the members of the Board who have no conflict of interest, who decide on the organisation of the investigation, engaging an external investigator where necessary.
9. A person whose reputation and qualifications raise no doubt as to their ability to properly implement the provisions of this Policy is appointed as the Responsible person.
10. No influence whatsoever may be exerted on the Responsible person implementing the requirements of the Policy, nor may they be otherwise hindered in performing the functions assigned to them by this Policy. Disciplinary penalties are applied for hindering the Responsible person in performing their functions.
11. The Responsible person, acting within the limits of their competence, performs the following functions:
    1. Ensures that the Channel operates continuously and is easily accessible to all Whistleblowers, including the periodic updating of information on the Company's intranet, website and other communication channels.
    2. Receives Reports through the Channel, decides whether a separate investigation team is needed for their investigation and, where necessary, initiates the issuing of an order on the formation of such a team, and ensures that the members of the investigation team are trained to work with confidential information and that they comply with the principles of the protection of Whistleblowers.
    3. Analyses the Information on an infringement received, investigates it or organises and coordinates the investigation, ensuring objectivity, impartiality and a timely response.
    4. Ensures the Confidentiality of the Whistleblower and protection against any adverse consequences related to the submission of the Report.
    5. Cooperates with Whistleblowers and Competent authorities by providing and/or receiving the necessary information.
    6. By 31 March of each year, submits to the Board a summary report on Reports, the results of their examination, compliance with time limits, systemic deficiencies and the implementation of corrective actions. Without delay, informs the members of the Board who have no conflict of interest of possible significant infringements, threats to clients' funds or to business continuity, or possible adverse action against the Whistleblower. Only the information necessary for the performance of their duties is provided, in compliance with the Confidentiality requirements.

7. Ensures that Information on an infringement submitted through the Company's Channel is accumulated and stored on a durable medium which can be reproduced where necessary, in accordance with the procedures approved internally by the Company. Anonymised data are used for statistical reporting; this does not replace the obligation to retain the documents of the examination of a Report in accordance with sub-point 36.5 of the Policy.
8. Performs other functions laid down in the Policy and in the LPW which are necessary for the effective examination of Reports and for ensuring the protection of Whistleblowers.

12. The Responsible person, in performing the functions assigned to them, has the right:
    1. to obtain the information and data they require from the Company's employees and units that are not subordinate to them and to demand their full cooperation, while ensuring Confidentiality. A refusal to cooperate with the Responsible person is considered to be a ground for a disciplinary penalty.
    2. when investigating Information on an infringement received through the Channel, to take decisions related to the conduct of the investigation which are binding on all employees and units of the Company.
    3. to document Information on an infringement submitted orally (during a face-to-face meeting) by drawing up accurate minutes of the conversation. In such a case, the Whistleblower is given the opportunity to check and correct the minutes of the conversation drawn up and to express their consent by signing them.

III. SUBMISSION OF A REPORT

13. The Company ensures that every Whistleblower has the possibility to report an Infringement through the Channel (as specified in sub-point 7.4 of the Policy) and encourages them to do so before applying to a Competent authority, if the Infringement can be effectively eliminated within the Company and if the Whistleblower considers that there is no risk of retaliation. However, it is emphasised that the Whistleblower has the right to apply to a Competent authority directly if there are reasonable concerns about possible adverse consequences or about ineffective examination of the internal Report, as provided for in the LPW.
14. The Whistleblower may submit Information on an infringement:
    1. through the Company's Channel;
    2. directly to a Competent authority;
    3. publicly (in compliance with the conditions laid down in the LPW).
15. The basis for submitting Information on an infringement is the data held by the Whistleblower or reasonable suspicions of a possible Infringement in the Company.
16. Information on infringements is submitted in respect of the following areas:
    1. danger to public safety or health, or to a person's life or health;
    2. danger to the environment;
    3. obstruction of, or unlawful influence on, investigations carried out by law enforcement institutions or on courts administering justice;
    4. infringements related to the prevention of the financing of unlawful activities, money laundering or terrorist financing;
    5. unlawful or non-transparent use of public funds or property;
    6. property acquired by unlawful means;
    7. concealment of the consequences of an Infringement committed, or obstruction of the determination of the extent of those consequences;
    8. infringements specified in the list approved by the Minister of Justice of the Republic of Lithuania, drawn up having regard to the scope of application of the European Union legal acts specified in Directive (EU) 2019/1937;
    9. damage 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 described in more detail in the related European Union measures;

10. infringements relating to the internal market, as referred to in paragraph 2 of Article 26 of the Treaty on the Functioning of the European Union, including infringements of the European Union competition and State aid rules, as well as infringements relating to the internal market in respect of acts which infringe corporate tax rules;
11. breaches of international sanctions implemented in the Republic of Lithuania or of restrictive measures laid down in the laws of the Republic of Lithuania;
12. other infringements relating to the public interest or posing a threat to the interests of the Company.

17. Time limits for the examination of Reports:
    1. The Company confirms to the person, by e-mail or by another means indicated in the Report, the receipt of the Report not later than 2 working days from the date of receipt of the Information on an infringement.
    2. The Responsible person takes a decision on the examination of the information not later than 5 working days from the date of receipt of the information and informs the Whistleblower thereof. Where it is decided not to examine the Report, the reasoned grounds are provided in writing.
    3. The Responsible person informs the Whistleblower of the results of the investigation and of the actions that have been taken not later than 3 months from the date of receipt of the Report. If, for objective reasons, the investigation cannot be completed within this time limit, the Whistleblower is informed thereof, with explanations provided and the anticipated completion date of the investigation indicated.
    4. The time limits laid down in this point 17 are binding for the Company’s internal procedure. Where legal acts lay down a shorter time limit for a specific action, the time limit laid down in the legal acts applies.
    5. The Company accepts, registers and, as far as objectively possible, investigates also those Reports which are submitted fully anonymously, in accordance with the same procedure as other Reports, including the time limit for taking a decision on the examination of the Report laid down in sub-point 17.2. Where the Whistleblower has not provided any contact details by which they could be contacted, the duties to inform the Whistleblower laid down in sub-points 17.1–17.3 and 25.4 (to confirm receipt of the Report and to inform them of the decision taken, of the results of the investigation or of the forwarding of the Information on an infringement to a Competent authority) do not apply, since it is objectively impossible to perform them; this fact is recorded in the Report assessment card.
18. A Whistleblower submitting Information on an infringement through the Channel is not required to be fully convinced of the veracity of the facts reported. They are under no obligation to assess whether the Infringement being reported meets the elements of criminal acts or of other legal infringements, as they are defined in legal acts and/or the Company’s regulatory acts. It is sufficient to have reasonable grounds to believe that an Infringement may be being committed.
19. The Company guarantees Confidentiality to the Whistleblower in all cases where Information on infringements is reported, irrespective of the outcome of the investigation and of whether the reported facts have been confirmed. However, Confidentiality is not guaranteed if the Whistleblower knew that the information submitted was false, that is, if they submitted knowingly false information. Confidentiality may also not be ensured if the Whistleblower requests in writing that their identity be disclosed. A Whistleblower who has submitted knowingly false information is liable in accordance with the procedure laid down in legal acts. Protection and Confidentiality do not apply if the person who has submitted Information on an infringement discloses a State or official secret.
20. The mere fact that the information submitted does not correspond to reality (for example, the Whistleblower was unaware of the circumstances relating to lawful activities of the Company which appeared to them to be unlawful) is not assessed as false information, and the Whistleblower is not considered to have submitted knowingly false information.
21. A Report of an Infringement may be submitted in the following ways:

1. in person to the Responsible person;
2. by registered post to the Company's address: Pilaitės pr. 16, Vilnius, LT-04352 Lietuva, marked "Confidential. To the Responsible person";
3. by e-mail to reportingchannel@paysera.com (accessible only to the Responsible person);
4. via the electronic reporting form, the link to which is published in the places specified in point 5 of the Policy (the responses to the form, irrespective of the technical means by which they are transmitted or stored, are accessible only to the Responsible person; the form does not require the person submitting the Report to provide their e-mail address or to sign in, and providing the name, surname and contact details in it is optional, so a Report may be submitted through it anonymously – the consequences of such a Report are set out in sub-point 24.3 of the Policy);
5. applying by telephone is not provided for, in order to ensure maximum security and documentation.

22. When using the Channel, the Whistleblower submits Information on infringements by completing a Report of an Infringement in the established form (Annex No. 1 to the Policy; when the Report is submitted in the manner specified in sub-point 21.4 of the Policy – the electronic reporting form) or by a free-form Report which must contain the information specified in point 24 of the Policy.
23. Where Information on an infringement is submitted orally (directly to the Responsible person), it is the duty of the Responsible person to record all the necessary information specified in point 24 of the Policy, and the duty of the Whistleblower to make sure that the Information on infringements submitted has been accepted and recorded to the full extent desired, but to no lesser extent than that specified in point 24 of the Policy. The personal data requested in the Report form are necessary for identifying the Whistleblower when resolving questions concerning the granting of protection and/or remuneration for Information on infringements. These data are stored in accordance with the procedure and time limits laid down in sub-point 36.5 of the Policy.
24. When submitting a Report, the Whistleblower indicates:
    1. what Infringement has been committed, is being committed or is being prepared, by whom, when and in what manner;
    2. the date on which and the circumstances in which the Infringement became known;
    3. their name, surname, place of work and other contact details. The Whistleblower may choose not to provide them and to submit the Report anonymously, but this may complicate the investigation process. Where no contact details at all are provided, no reply will be given to the Whistleblower – neither confirmation of receipt of the Report nor information on the decision taken and on the results of the investigation (sub-point 17.5 of the Policy) – and the Responsible person will not be able to request additional information. The protection, encouragement and assistance measures laid down in Article 8 of the LPW apply to a person who has submitted a Report anonymously in cases where their identity has been disclosed and it is necessary to protect them against adverse consequences (paragraph 6 of Article 3 of the LPW);
    4. where possible, any documents, data or information held that disclose the elements of a possible Infringement.
25. Having received Information on an infringement through the Responsible person, the Company must:
    1. assess whether the Information on an infringement complies with the provisions of the Policy and of the LPW;
    2. verify whether the Information on an infringement submitted is sufficient for the commencement of an investigation;
    3. register the Report in a specially designated electronic system or electronic register, ensuring Confidentiality and the security of all related data and their accessibility only to authorised persons;
    4. where it is established that the Company is not competent to assess this information, forward it to a Competent authority not later than 2 working days from the date of receipt of the Information on an infringement and inform the Whistleblower thereof.

IV. APPLYING TO COMPETENT AUTHORITIES

26. A Whistleblower who has submitted Information on infringements may, in respect of the adverse consequences that they may suffer or are suffering in connection with the submission of the information, consult a Competent authority regarding the means or measures for the defence of their rights. In addition, pursuant to paragraph 3 of Article 11 of the LPW, the Whistleblower may apply to a Competent authority regarding the granting to them of the status of Whistleblower (as defined in paragraph 8 of Article 2 of the LPW).
27. A Whistleblower may apply directly to a Competent authority regarding an Infringement where at least one of the following circumstances exists:
    1. the Infringement is of essential significance to the public interest;
    2. it is necessary to prevent or terminate the Infringement as soon as possible, because major damage may occur;
    3. persons in managerial positions or persons connected with the Company by employment, service or contractual relations may themselves be committing or have committed Infringements;
    4. Information on an infringement was submitted through the Channel, but no reply was received, or no action was taken in response to the information submitted, or the measures that were taken were ineffective;
    5. there are grounds to believe that, upon submission of the information through the Channel, the anonymity or Confidentiality of the Whistleblower may not be ensured, that attempts will be made to conceal the reported Infringement or that the Whistleblower will be subjected to adverse consequences;
    6. there is no functioning Channel in the institution;
    7. the Whistleblower cannot use the Channel because they are not connected with the Company by employment, service or other legal relations;
    8. they become aware of possible elements of criminal acts that are being prepared, are being committed or have been committed.
28. Where the Whistleblower has not received a reply, or where no action has been taken in the Company in response to the information submitted, or where the measures taken are insufficient to prevent the Infringement, they have the right, pursuant to point 4 of paragraph 4 of Article 4 of the LPW, to apply directly to a Competent authority and to submit a Report in accordance with point 29 of the Policy.
29. The Whistleblower applies to a Competent authority by a Report in the form approved by that authority or in free form, indicating that the Report is being submitted pursuant to the national legal acts implementing Directive (EU) 2019/1937 (in Lithuania – the LPW).
30. When submitting Information on an infringement or a Report, the Whistleblower indicates:
    1. the specific factual circumstances of the Infringement;
    2. the person who is preparing to participate, is participating or has participated in the commission of the Infringement;
    3. whether they have already reported this Infringement; if they have reported it – to whom it was reported and whether a reply was received;
    4. their name, surname, personal identification number or date of birth (if they do not have a personal identification number) and contact details.
31. Where possible, the Whistleblower attaches written or other data held 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 an infringement may be submitted publicly where:
    1. the Whistleblower first submitted the Report through the Channel and/or to a Competent authority, but no appropriate action was taken in respect of their Report within the period specified in the Policy;

2. the Whistleblower has reasonable grounds to believe that the Infringement poses a danger to people's lives, public health or the environment, where urgent action is necessary in order to prevent such a threat.

34. In order to obtain the guarantees laid down in the law, a Whistleblower who has submitted information publicly must apply to a Competent authority with a request.
35. The provisions of paragraph 3 of Article 3 of the LPW, as well as the measure specified in point 2 of paragraph 1 of Article 8 of the law, do not apply to a Whistleblower who has submitted Information on an infringement publicly.

V. STORAGE OF INFORMATION ON INFRINGEMENTS AND ENSURING CONFIDENTIALITY

36. The Company ensures the Confidentiality of the content of the information received through the Channel and of other data enabling the Whistleblower to be identified by implementing the following measures:
    1. Access to Reports and to data on the identity of the Whistleblower is granted only to authorised persons to the extent necessary for their functions. IT administration rights (for example, the administration of the reportingchannel@paysera.com mailbox or of the electronic reporting form referred to in sub-point 21.4 of the Policy) do not in themselves confer the right to access the content of Reports. Technical access rights are restricted, and their use is logged and monitored. The obligation of Confidentiality continues after the expiry of the person's powers.
    2. The Responsible person ensures that the Information on infringements received and the related data (information, documents) are kept securely and that they may be accessed only by those persons examining the Information on infringements who have such a right (for example, employees appointed to carry out a specific investigation or members of a commission).
    3. The Responsible person, in so far as this is possible, depersonalises the data and separates data capable of identifying the Whistleblower, storing such data separately from the investigation file.
    4. The file of the investigation of the Information on infringements is marked with the Confidentiality marking "Confidential" together with the other information classification and distribution restriction markings established within the Company. The Confidentiality of the investigation file is ensured irrespective of the results of the investigation of the Information on infringements received.
    5. Upon completion of the investigation of the Information on infringements, the entire file is kept for not less than five years, as prescribed by paragraph 1 of Article 7 of the LPW, and for not longer than ten years, unless an instruction of a Competent authority is received. The file is destroyed in accordance with the procedures approved internally by the Company. The destruction of the file does not mean the declassification of the information, unless the Whistleblower has waived the ensuring of Confidentiality in writing or the information has lawfully become public.
    6. The file of a completed investigation is archived with restricted access. Access is granted only to authorised persons who need the file in order to perform their lawful functions. Access rights are reviewed when the person's duties or powers change. Documents are archived in accordance with the rules approved within the Company.
    7. Information is transferred to institutions authorised to investigate infringements on the grounds laid down by legal acts and to the extent necessary. The Whistleblower is informed of the transfer of data disclosing their identity in accordance with the procedure and within the time limits laid down by legal acts. The legal basis, the recipient and the scope of the transfer, and any exception to the obligation to inform that was applied, are documented.
37. The Company, having obtained the Whistleblower's consent, has the right to record the receipt of Information on an infringement in one of the following ways:

1. to save a recording of the conversation on a durable medium from which the information sought can be retrieved;
2. to process the information in accordance with the precise meeting minutes form drawn up by the Responsible person.

VI. PROHIBITION OF ADVERSE ACTION

38. From the day of the submission of the information, it is prohibited to take any adverse measures against the Whistleblower, and likewise to threaten to apply them or to attempt to do so, including, but not limited to:
    1. temporarily suspending them from their duties;
    2. dismissing them from work or service;
    3. suspending promotion to a higher position;
    4. demoting them to a lower position or transferring them to another workplace;
    5. failing to convert a fixed-term employment contract into an open-ended employment contract where the employee has legitimate expectations that permanent work will be offered to them;
    6. failing to renew a fixed-term employment contract, or terminating a fixed-term employment contract early;
    7. intimidating them;
    8. using coercion;
    9. harassing them;
    10. restricting the opportunity to participate in previously customary formal or informal activities, or excluding them from such activities;
    11. discriminating against them;
    12. threatening retaliation;
    13. restricting career opportunities or suspending training;
    14. reducing wages;
    15. unjustifiably changing working time, or unjustifiably assigning additional tasks or transferring them to other persons;
    16. raising doubts about competence;
    17. assessing performance results negatively or providing a negative reference about the employee;
    18. passing on to third parties negative information about them, as a result of which the person may in future be unable to find work in that sector or industry;
    19. revoking the right to work with information constituting a State or official secret;
    20. imposing or applying any disciplinary penalties or other sanctions (including financial ones);
    21. causing harm (including harm to the person’s reputation, in particular on social networks);
    22. causing financial losses (including the loss of business and income);
    23. terminating a contract for the supply of goods or the provision of services early;
    24. revoking the validity of a licence or permit;
    25. referring them to psychiatrists or to other medical specialists;
    26. applying any other adverse measures.
39. The prohibition of adverse action against the Whistleblower applies to the employer and to other employees of the Company.
40. It is likewise prohibited to take adverse action against:
    1. family members and relatives of the person submitting the Information on an infringement;
    2. colleagues working at the Company or at another legal person linked to the Company by relations of subordination, at which they may suffer adverse consequences on account of the submission of the Information on an infringement;
    3. Assistants who help in the process of submitting Information on an infringement obtained in

work-related circumstances;
4. legal persons which are the property of the person who submitted the Information on an infringement, or for which that person works, or with which that person is otherwise connected in work-related circumstances.

41. If the Whistleblower considers that adverse action is being taken against them on account of the submission of the Report, the Company must prove that the actions were motivated by objective reasons unrelated to the Report.
42. If the Whistleblower considers that adverse action is being taken against them, they may:
    1. apply to the Responsible person (where the adverse action is not being taken by the Responsible person);
    2. apply to the Company's manager or to the Board;
    3. apply to a Competent authority;
    4. make use of other legal remedies provided for by legal acts.

VII. REMUNERATION TO WHISTLEBLOWERS FOR VALUABLE INFORMATION

43. By decision of the Company's manager, remuneration may be awarded for valuable Information on infringements submitted to the Responsible person (that is, to the Company).
44. Remuneration in this Policy is understood as a one-off monetary payment for valuable Information on infringements submitted to the Responsible person (that is, to the Company).
45. Remuneration may be awarded to the Whistleblower only where all of the following conditions are present:
    1. The Information on an infringement submitted by the Whistleblower is considered valuable where it has helped to prevent possible major pecuniary damage or has made it possible to prevent, terminate or investigate a criminal act.
    2. The remuneration awarded to the Whistleblower by decision of the Company is an independent decision of the Company and does not depend on the Competent authority deciding on the award of remuneration on behalf of the State.
    3. The operation of paying out the remuneration may not breach the Whistleblower's Confidentiality, or disclose that remuneration is being paid for a Report of an Infringement or that the recipient is the Whistleblower, unless the Whistleblower has waived the ensuring of Confidentiality in writing.
46. The amount of the remuneration is determined by the Company's manager, taking into account the following factors:
    1. the value of the information and its impact on the Company;
    2. the extent of the damage avoided;
    3. the level of the Whistleblower's cooperation during the investigation;
    4. other significant circumstances.
47. The remuneration is paid out confidentially, in order to protect the identity of the Whistleblower.

VIII. PREVENTIVE MEASURES, TRAINING AND MONITORING

48. The Company's commitments and principles of prevention:
    1. The Company adheres to a zero-tolerance policy towards any form of retaliation or adverse action in respect of Whistleblowers.
    2. The Company's managers at all levels are personally responsible for creating a safe environment based on trust. They are expected to set a personal example, to encourage open discussions and to respond promptly to the first signs of inappropriate conduct.

49. The Company organises mandatory training on the Whistleblower protection system, the recognition of Infringements and the operation of the internal Channel:
    1. Training is organised periodically, not less frequently than once every 2 (two) calendar years.
    2. Newly recruited employees are given the opportunity to familiarise themselves with the Policy and the training material not later than 1 (one) month from the start of their work.
    3. The fact of participation in training is recorded in the Company's internal systems.
50. Independent monitoring and control of the implementation of this Policy is carried out by the Monitoring Unit. It ensures supervision of the process of administering Reports which is carried out by the Responsible person and assesses whether the Responsible person complies with the established time limits, whether the Confidentiality of the data is ensured and whether the Whistleblower protection measures are effective. Where the Responsible person performs the risk and compliance management function, independent monitoring and control of the implementation of this Policy is carried out by the unit or entity performing the internal audit function, including an external service provider. Persons carrying out monitoring do not assess processes they have administered or Reports they have examined. Where independence cannot be ensured within the Company, an independent external assessor is engaged. Significant findings and progress in implementing recommendations are submitted to the Board.

IX. FINAL PROVISIONS

51. The Whistleblower is liable for damage arising from the submission of the information only where it is proved that they could not reasonably have believed that the Information on an infringement being submitted was correct, that is, that they acted intentionally in submitting false information.
52. Other protection, encouragement and assistance measures which are not set out in this Policy are established in the LPW and in other legal acts enshrining the protection of Whistleblowers.
53. The Legal Unit reviews the Policy not less frequently than once every two years and, where necessary, initiates its amendment, taking into account changes in the legal acts of the Republic of Lithuania and of the European Union, practical experience in applying the Policy within the Company, and the good practices of financial market participants.
54. This Policy comes into force on the day of its approval. The Policy, its annexes and information about the reporting channels are permanently published on the Company's intranet and are publicly available on the Company's website www.paysera.lt.

WHISTLEBLOWING POLICY (valid until 2026.10.21)

WHISTLEBLOWING POLICY (valid until 2026.08.19)