Table of contents

1. Legal basis and purpose of the procedure

1.1. The purpose of introducing the internal reporting and follow-up procedure (hereinafter referred to as the Procedure or the Internal Reporting Procedure) is the need and necessity to ensure that the Company implements the requirements set out in the Whistleblower Protection Act of 14 June 2024 (Journal of Laws 2024, item 928). Receiving reports of breaches of law constitutes part of proper and safe management at Europa Systems sp. z o.o. (hereinafter referred to as the Company) and serves to increase the effectiveness of detecting irregularities as well as taking action to eliminate them and reduce risks at all organisational levels.

1.2. The Internal Reporting Procedure was established after consultation with representatives of the Company's workforce, selected in accordance with the Company's procedure.

1.3. The purpose of the actions set out herein shall include, in particular:

1.3.1. setting up a reporting system at the Company by creating secure reporting channels;

1.3.2. ensuring a high level of protection for whistleblowers, preventing any retaliation against them;

1.3.3. defining the material scope of application of the provisions hereof, including the types and areas to be reported;

1.3.4. defining roles and responsibilities in the implementation of the reporting and follow-ups;

1.3.5. providing secure channels for whistleblowers to report breaches of the law;

1.3.6. laying down rules on the reporting procedure, with particular regard to the protection of whistleblowers;

1.3.7. defining rules relating to data collection and recording, including record-keeping;

1.3.8. ensuring transparency in the follow-ups;

1.3.9. developing and implementing a formal process for reporting and following up on breaches of law.

2. Scope of the Internal Reporting Procedure

2.1. Each person providing services to the Company (irrespective of the type and form of employment) shall be required to read and comply with the Internal Reporting Procedure.

3. Definitions

3.1. Follow-up – shall mean an action taken by the Company in order to assess the veracity of the information contained in a report and to counteract a reported breach of law, in particular by means of an investigation, initiation of control or administrative proceedings, prosecution, action taken to recover funds or closure of a procedure carried out under the internal procedure for reporting breaches of law and taking follow-ups or the procedure for receiving external reports and taking follow-ups.

3.2. Retaliation – shall mean a direct or indirect act or omission in a work-related context that is caused by a report or public disclosure and that violates or is likely to violate the whistleblower's rights or causes or is likely to cause unwarranted harm to the whistleblower, including the unwarranted initiation of proceedings against the whistleblower.

3.3. Information on a breach of law – shall mean information, including a reasonable suspicion of an actual or potential breach of law, which has occurred or is likely to occur in a Company where the whistleblower has participated in the recruitment process or other pre-contractual negotiations, has worked, or in another legal entity with which the whistleblower has had contact in a work-related context, or information concerning an attempt to conceal such a breach of law.

3.4. Feedback – shall be understood as the provision of information to the whistleblower on the follow-ups planned or taken and the reasons for such actions.

3.5. Work-related context – shall be understood as past, present or future work-related activities under an employment or other legal relationship constituting the basis the provision of work or services or functions in the Company, where the information on a breach of law has been obtained and the possibility of experiencing retaliation exists.

3.6. Breach of law – shall be understood as acts or omissions which are unlawful or intended to circumvent the law in the context of the subject areas referred to in paragraph 5.1. hereof.

3.7. Public authority – it should be understood as chief and central government administration bodies, field government administration bodies, bodies of local government units, other state bodies and other entities performing public administration tasks under the law, competent to take follow-ups in the areas indicated in paragraph 5.1. hereof.

3.8. Person affected by the report– shall be understood to mean a natural person, a legal person or an organisational unit without legal personality, to which the law confers legal capacity, identified in report or public disclosure as a person who has committed a breach of law, or as a person with whom the person who has committed the breach of law is associated.

3.9. Facilitator – shall mean an individual who assists a whistleblower with a report or public disclosure in a work-related context and whose assistance should not be disclosed.

3.10. Person associated with the whistleblower – shall mean an individual who may experience retaliation, including a co-worker or family member of the whistleblower.

3.11. Whistleblower/Reporting Person – shall be understood as an individual who reports or publicly discloses information on a breach of law obtained in a work-related context, including in particular: an employee, a temporary employee, a person providing work on a basis other than employment relationship, including under a civil law contract, an entrepreneur, a proxy, a shareholder, a partner, a member of a body, a person providing work under the supervision and direction of a contractor, subcontractor or supplier, an intern, a volunteer, an apprentice.

3.12. Public disclosure – shall be understood as providing information on a breach of law public.

3.13. Report – shall be understood as an oral or written internal report or an external report, provided in accordance with the requirements set out in the legislation currently in force.

3.14. Internal report – shall mean the oral or written information on a breach of law to the Company.

3.15. External report – shall be understood to mean the oral or written information to the Ombudsman or a public authority of a breach of law.

4. Roles and responsibilities

4.1. Reporting Person – the person reporting a potential breach of law, who is responsible for providing accurate and as complete information as possible on the reported breach of law, thus enabling a full and thorough follow-up.

4.2. Compliance Officer – an employee of the Company appointed by a Resolution of the Management Board who is responsible for the initial assessment, review, giving an opinion on the application, anonymising personal data where warranted, and leading the follow-up. It is also the responsibility of the Compliance Officer to communicate information and findings after the initial assessment of the report, to co-organise meetings on the ongoing follow-up report and to liaise with the Reporting Person and the staff assisting in the investigation of the reported potential breach of law.

4.3. Team – a team acting in an impartial, independent manner, on the basis of a mandate to receive reports and follow up, consisting of: Compliance Officer, General Counsel and Director of Human Resources, hereinafter referred to as permanent members. Depending on the nature and extent of the reported breach of law and in justified cases, the Team shall be joined, at the request of the Compliance Officer, by a Company's employee whose presence on the Team will be necessary to carry out the explanation of the reported breach of law. The Team shall be responsible for receiving the reports and shall have an overall oversight of their reception. It shall also be responsible for internal investigation and follow-up.

4.4. Business process owners/managers of the Company's organisational units – responsible for supporting the Team's activities, including providing Team members with all information related to the Team's internal investigation.

4.5. Management Board of the Company – responsible for adopting and implementing the

Procedure, ordering the preparation and delivery of training on the subject matter hereof, as well as for taking the necessary actions (including disciplinary actions) arising from the conclusions of the Team and, where appropriate, ordering the information of the relevant external (public) authorities.

5. Manners of providing internal reports

5.1. Reports should relate to the following categories of breaches of law:

5.1.1. corruption;

5.1.2. public procurement;

5.1.3. financial services, products and markets;

5.1.4. anti-money laundering and countering the financing of terrorism;

5.1.5. product safety and compliance;

5.1.6. transport safety;

5.1.7. environmental protection;

5.1.8. radiological protection and nuclear safety;

5.1.9. food and feed safety;

5.1.10. animal health and welfare;

5.1.11. public health;

5.1.12. consumer protection;

5.1.13. privacy and data protection;

5.1.14. security of ICT networks and systems;

5.1.15. financial interests of the State Treasury of the Republic of Poland, a local government unit and the European Union;

5.1.16. European Union internal market, including public law competition and state aid rules and corporate taxation;

5.1.17. constitutional freedoms and rights of man and citizen.

5.2. An internal report may relate to a reasonable suspicion of an actual or potential breach of law that has occurred or is likely to occur within the Company.

5.3. The Reporting Person may make an internal report through the following channels:

5.3.1. dedicated IT form located on the Company's website at: https://europasystems.pl/;

5.3.2. at the e-mail address – naruszenia@europasystems.com;

5.3.3. orally during a face-to-face meeting with the Team within 14 days of receiving such a request. With the consent of the Reporting Person, the internal oral report will be documented in the form of:

a) a searchable recording of the conversation, or

b) an accurate transcription of the conversation, or

c) protocol of the interview, reproducing its exact course.

5.4. In the case of an agreement to document the oral internal report, the Reporting Person may review, correct and approve the interview transcript or interview protocol by signing it.

5.5. Regardless of the communication channel chosen, the Reporting Person shall be guaranteed full confidentiality of the information and security of the personal data of the whistleblower and the third party indicated in the report. The protection of confidentiality shall apply to information from which the identity of such persons can be directly or indirectly identified. The Reporting Person's personal data allowing for the identification of the Reporting Person shall not be disclosed to any person not authorised to receive and process reports, unless the Reporting Person consents to such disclosure. Any personal data not demonstrably relevant to the processing of the internal report shall not be collected and, if provided, shall be deleted immediately. The deletion of these personal data shall take place within 14 days of the determination that they are not relevant to the case. Maintaining confidentiality is intended to guarantee the Reporting Person's sense of security and to minimise the risk of retaliation. The Reporting Person who has made a report and whose personal data have been unauthorisedly disclosed should immediately notify the Team of the situation. The Team shall be obliged to take measures to protect the Reporting Person. The identity of the Reporting Person as well as all personally identifiable information shall not be disclosed to the subjects of the report, to third parties or to other employees and associates of the subject. The identity of the Reporting Person as well as other information enabling his/her identification may only be disclosed if such disclosure is a necessary and proportionate obligation under generally applicable law in the context of investigations or preparatory proceedings or judicial proceedings conducted by public authorities or courts, respectively. The identity of the entities to which the report relates shall be subject to confidentiality requirements to the same extent as the identity of the Reporting Person.

5.6. The report should contain as much information as possible, including a clear and complete explanation of the subject matter of the internal report, in order to enable the follow-up Team to conduct an internal investigation. The report should include, in particular:

5.6.1. the date and place where the breach of law occurred or the date and place where information on a breach of law was obtained;

5.6.2. information on the breach of law (description of the problem/situation, provision of relevant information and circumstances, basis for reporting the breach);

5.6.3. indication of the person(s) affected by the report (identity, function, place of work), if possible;

5.6.4. identification of a possible victim;

5.6.5. identification of possible witnesses to the breach of law;

5.6.6. indication of any evidence available to the Reporting Person, other information in his/her possession (e.g. documents/materials) relating to the reported breach of law that may be helpful in the process of dealing with the report;

5.6.7. data of the Reporting Person (in case the Reporting Person decides to disclose it or it becomes necessary due to a specific legal basis);

5.6.8. indication of preferred method of feedback contact.

5.7. In the case of a report of a breach of law in an anonymous manner (without providing details, including contact details), the Team does not confirm to the whistleblower the fact that an internal report has been accepted, however, the Team may decide to continue the investigation and follow-up in the manner set out herein, or may leave the internal report without further

recognition in the absence of details for investigation and follow-up.

5.8. The report can only be made in good faith. Pursuant to the wording of the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws of 2024, item 928), a person making a report of false information is subject to a fine, the penalty of restriction of liberty or imprisonment for up to two years.

5.9. If it is determined, either as a result of the analysis of the internal report or during the course of the investigation, that the internal report knowingly contains untruths or conceals the truth, the Reporting Person may be held liable for the disciplinary liability set out in the Labour Code. Such behaviour can also be qualified as a grave breach of fundamental employment duties and as such result in termination of the employment contract without notice. In the case of a person providing labour, services or goods under a civil law contract, the submission of a false declaration may result in termination of the contract and the cooperation. A person who has made a report in which the truth has been knowingly misrepresented or concealed does not benefit from the protection provided for Whistleblowers.

6. Rules for handling internal reports on breaches of law and follow-ups

6.1. Once an internal report has been made by the Reporting Person via the dedicated contact form or e-mail box, an acknowledgement shall be sent to the Reporting Person within 7 days of receipt, unless the Reporting Person has not provided a contact address to which the acknowledgement should be forwarded. In the case of a verbal report, the Reporting Person shall receive confirmation of acceptance at the meeting at which the report is made.

6.2. Upon receipt of the report, the Compliance Officer, who has the duty to continuously monitor the communication channels for reporting violations of the law, reviews, shall give an opinion and make a preliminary assessment of the report. At this stage, a possible anonymisation of personal data (if necessary), the processing of which, in the opinion of the Compliance Officer, is not relevant to the report under consideration, shall take place before the report is forwarded for further processing.

6.3. The Compliance Officer, in the next step, shall forward the preliminary conclusions and the content of the internal report to the other permanent members of the Team, assigning the report a category of breach in accordance with paragraph 5.1. hereof.

6.4. Upon receipt of the internal report, the Team shall take steps to assess the veracity of the information contained in it, including verification of the internal report. The Compliance Officer shall conduct further communication with the Reporting Person, including, if reasonable requesting additional information on the internal report and providing feedback on the report.

6.5. The Team may decide not to conduct an investigation where the content of the internal report shows that it is indisputably false or it is impossible to obtain the information necessary for the investigation.

6.6. The internal report that allows for an investigation shall be subject to immediate processing.

6.7. If the internal report is not qualified for further processing due to insufficient data, the follow-up Team shall have the right to ask questions and obtain additional information on the subject of the action being carried out, and persons called upon to provide answers or documents or materials shall be obliged to provide such answers or documents or materials without delay. If the necessary data is not completed within thirty days, the internal report shall not be further processed, of which the Compliance Officer shall inform the Reporting Person in a separate communication sent to the contact address indicated by the Reporting Person.

6.8. The Team may involve, if it considers it appropriate, representatives of the Company's business units or independent consultants to participate in the investigation.

6.9. The Team shall retain full autonomy and, in conducting the follow-up, objectively assesses the material received and decide how to proceed with each reported breach of law. Meetings shall be protocoled/recorded by the Compliance Officer in the form of a memo accepted by the Company and the said memo shall be attached to the pending report.

6.10. Following the investigation, the Team shall assess the validity of the internal report. In the case of a legitimate internal report, the Team shall issue a report recommending appropriate corrective or disciplinary action against the person who committed the breach of law. The report should also contain recommendations aimed at eliminating and preventing identical or similar violations to those described in the internal report in the future.

6.11. If the material collected by the Team is not sufficient to conclude the investigation, the Team shall have the right to ask questions and obtain additional information on the subject of the ongoing follow-up. Persons called upon to respond or provide documents or materials shall be obliged to respond or provide the relevant documents or materials without undue delay.

6.12. The report drawn up by the Team shall be forwarded to the Management Board of the Company, which, if necessary, shall decide to take disciplinary, training or procedural action, or has the case resulting from the investigation prepared and reported to the appropriate external (public) authority.

6.13. The Team shall recognise the internal report, follow up, provide feedback without undue delay, no later than 3 months after the acknowledgement of the internal report or, if no acknowledgement of the internal report is provided, within 3 months after the expiry of 7 days of the internal report.

7. Collection and recording of the Team follow-up

7.1. The Company shall keep a register of internal reports. Each internal report should be recorded by the Compliance Officer in the register of internal reports, regardless of the course of the follow-up. The Compliance Officer shall be responsible for keeping the

register of internal reports. A template of the register of reports is appended as Appendix 1 hereto.

7.2. The register of reports shall contain at least:

7.2.1. report number;

7.2.2. subject of the breach of law;

7.2.3. personal data of the Reporting Person and of the persons affected by the report, necessary to identify them;

7.2.4. Reporting Person's contact address;

7.2.5. date of the internal report;

7.2.6. information on follow-ups taken;

7.2.7. date of completion of the case.

7.3. The register of reports shall be kept confidential. Personal data and other information in the register of internal reports shall be retained for a period of 3 years after the end of the calendar year in which the follow-ups have been completed or the proceedings initiated by those actions have been completed or the reports has been forwarded to the public authority competent to take follow-up.

7.4. The necessary information on the internal report relating to the Company's IT security, for the purpose and scope of preventing data leakage and securing the organisation, should be immediately forwarded to the IT department.

7.5. Internal reports of a personal data breach must be immediately forwarded to the Data Protection Officer in order to carry out the appropriate investigation as defined in the provisions of the GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: GDPR) (Official Journal of the EU L119/1).

7.6. If the Team deems an internal report to be unsubstantiated, all data collected, including personal data and information, shall be subject to deletion within 36 months of the Team deeming the internal report to be unsubstantiated.

7.7. If an internal follow-up results in corrective action but does not involve the Reporting Person or the person affected by the report, all personal data and information obtained as part of the internal report will be deleted within 36 months after completion and positive verification relating to the implementation of the corrective action.

7.8. If an internal follow-up results in action being taken against the person affected by the report (including disciplinary action) or termination of employment, all personal data and information obtained as part of the internal report shall be deleted within 36 months

of the termination of employment or after any claims by either party relating to the action have ceased.

7.9. If an internal follow-up results in a report to a competent external (public) authority, any personal data and information obtained as part of the report shall be deleted no sooner than after the conclusion of the matter with the competent external authority, subject to the cessation of any claims by either party relating to that action.

8. External reporting

8.1. The Whistleblower may make an external report without first making an internal report.

8.2. The external report is received by the Ombudsman or an external (public) body in the manner specified by the Ombudsman or an external (public) body and, where appropriate, to the institutions, bodies or agencies of the European Union in the procedure for the receipt and follow-up of external reports, which lays down in particular the procedure for dealing with information on infringements reported anonymously, hereinafter referred to as the “external report procedure”.

8.3. The Ombudsman and the public body shall be separate controllers in respect of the personal data provided in the external report accepted by these bodies.

8.4. All information relating to external reporting is posted on the relevant page of the Public Information Bulletin of the Ombudsman or public body.

9. No retaliation

9.1. It shall be prohibited to retaliate, attempt to retaliate or threaten to retaliate or threaten to retaliate against a Whistleblower who has made a report, as well as public disclosure – in accordance with the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws of 2024, item 928).

9.2. Retaliation against the facilitator and against the person who is associated with the Whistleblower shall be prohibited.

9.3. Taking any action of a repressive, discriminatory nature or any other kind of unfair treatment against the Whistleblower shall be treated as a breach of the Procedure, and may result in disciplinary liability or termination of the contract that binds the person taking the retaliatory action to the Company.

9.4. In particular, it shall be unacceptable in relation to the Whistleblower:

9.4.1. to refuse to establish an employment relationship;

9.4.2. to terminate or termination without notice the employment;

9.4.3. not to conclude a fixed-term employment contract or an indefinite employment contract after termination of the probationary contract;

9.4.4. not to conclude a further fixed-term employment contract or to conclude an

indefinite-term employment contract following the termination of a fixed-term contract – where the employee had a legitimate expectation that such a contract would be concluded with him/her;

9.4.5. to reduce remuneration for work;

9.4.6. to withhold promotion or miss someone in promotion;

9.4.7. to miss someone in the award of work-related benefits other than wages or reduction in the value of such benefits;

9.4.8. to transfer an employee to a lower position;

9.4.9. to suspend from employment or official duties;

9.4.10. to transfer to another employee the existing employment duties;

9.4.11. to make adverse change in the place of work or working time schedule;

9.4.12. to make negative performance appraisal or give negative job opinion;

9.4.13. to impose or apply a disciplinary measure, including a financial penalty, or a measure of a similar nature;

9.4.14. to coerce, intimidate or exclude;

9.4.15. to bully;

9.4.16. to discriminate;

9.4.17. to apply adverse or unfair treatment;

9.4.18. to withhold participation or miss someone from typing for professional qualification training;

9.4.19. to unjustifiably refer for medical examination, including psychiatric examination, insofar as separate regulations provide for the possibility of referring an employee for such examination;

9.4.20. to undertake action to make it more difficult to find future employment in a particular sector or industry on the basis of an informal or formal sectoral or industry agreement;

9.4.21. to cause financial loss, including economic loss or loss of income;

9.4.22. to inflict other non-material damage, including infringement of personal rights, in particular of the Reporting Person’s good name.

9.5. Retaliation for making a report or public disclosure shall also be deemed to be a threat or attempted measure as set out in paragraph 9.4 above. The Employer shall have the burden of proving that the action taken is not retaliatory.

9.6. A Whistleblower who makes a report in bad faith (i.e. who makes a report knowing that no breach of law has occurred) shall not be subject to the protection provided for in the Procedure and in the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws of 2024, item 928).

9.7. A person who has suffered damage due to a so-called bad faith report has the right to claim compensation or damages for the breach of personal rights from the Reporting Person who made such report.

10. Security and protection of personal data

10.1. The processing of personal data obtained in the activities described in the provisions of this Procedure shall be carried out in accordance with the applicable legislation, in particular:

10.1.1. Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of whistleblowers;

10.1.2. Act of 14 June 2024 on the protection of whistleblowers;

10.1.3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation);

10.1.4. Act of 10 May 2018 on the protection of personal data.

10.2. Only persons authorised to do so in accordance with this Procedure and persons whose access to the data results from current legislation shall have access to the data contained in the reports and the related documentation and reports.

10.3. The Reporting Person is protected from possible retaliation in accordance with Article 19 of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of whistleblowers and the provisions of Chapter 2 of the Act of 14 June 2024 on the protection of whistleblowers.

10.4. The person affected by the report is protected in accordance with Article 22 of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of whistleblowers and the provisions of Chapter 2 of the Law of 14 June 2024 on the protection of whistleblowers.

10.5. Only persons authorised in writing by the Company may be permitted to receive and verify internal reports, follow up and process the personal data of the Reporting Person and the person affected by the report. Authorised persons are obliged to maintain secrecy with regard to the information and personal data they have obtained in the course of accepting and verifying internal reports, and to take the follow-up, even after the termination of the employment relationship or other legal relationship under which they performed this work.

11. Exception management

11.1. Any deviation from the adopted Procedure for making reports on breaches of law and taking the follow-up shall be handled through the exception management process, with each report of a deviation requiring an expert assessment by the reporting person to analyse the possible risks and countermeasures applied, as well as the submission of a business case.

11.2. The Management Board of the Company, after taking into account the opinion of the Compliance Officer, shall decide whether to accept or reject the variance request submitted.

12. Review and monitoring of changes and final provisions

12.1. The Compliance Officer shall be responsible for the adequacy and effectiveness of the operation of the Procedure.

12.2. An assessment of the adequacy and effectiveness of the Procedure shall be made at least annually by the Compliance Officer.

12.3. The line supervisor shall be responsible for familiarising all subordinate employees with the provisions of the Procedure.

12.4. The Compliance Officer shall be responsible for regular training on the scope of the Procedure.

12.5. The Procedure shall come into effect on 25 September 2024, that is, seven days after it has been made known to those performing the work, in the manner adopted by the Company.

12.6. The Procedure shall be made available on SharePoint (Group_ISO_9001) and on the Company's website.

13. Related documents

BZAR – 02 Appendix 1 Register of reports