INTERNAL REPORTING PROCEDURE
at Sescom S.A.
(hereinafter referred to as the "Procedure")

1. Objective

Sescom S.A. strives to counteract violations of the law that may negatively affect the public interest and the proper functioning of the organization. In connection with the above, the Internal Reporting Procedure for whistleblowers is introduced, i.e. for people who have justified concerns about improper conduct at Sescom S.A.

This Procedure aims to create safe and effective channels for reporting violations of the law, to establish appropriate follow-up actions, and to protect those who report such violations from possible retaliation.

By introducing this Procedure, Sescom S.A. undertakes to systematically monitor reported irregularities and ensure appropriate protection for persons reporting violations, protection of personal data and protection against retaliatory actions. The implementation of these commitments is aimed at creating a safe working environment, in compliance with applicable legal regulations, which contributes to maintaining corporate responsibility standards.

The implementation of the Procedure is an element of the implementation of the obligations imposed by Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on persons reporting violations of Union law (OJ EU L No. 305, p. 17, as amended) and national legal regulations, i.e. Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws, item 928).

2. Definitions

2.1. **Company** – Sescom S.A. with its registered office in Gdańsk (80-244), aleja Grunwaldzka 82, entered into the Register of Entrepreneurs of the National Court Register maintained by the District Court of Gdańsk-Północ in Gdańsk, 7th Commercial Division under the KRS number: 0000314588, NIP: 9571006288, REGON: 220679145, with the share capital of PLN 2,280,524, fully paid up.

2.2. **Reporting Party** – a natural person who reports or publicly discloses information about a violation of the law obtained in a work-related context, including: an employee; a temporary employee; a person performing work on a basis other than an employment relationship, including under a civil law contract; an entrepreneur; a proxy; a shareholder or partner; a member of a body of a legal person or an organizational unit without legal personality; a person performing work under the supervision and management of a contractor, subcontractor or supplier; a trainee; a volunteer; an apprentice; an officer within the meaning of Article 1 section 1 of the Act of 18 February 1994 on the pension provisions for officers of the Police, Internal Security Agency, Intelligence Agency, Military Counterintelligence Service, Military Intelligence Service, Central Anticorruption Bureau, Border Guard, Marshal's Guard,

State Protection Service, State Fire Service, Customs and Tax Service and Prison Service and their families (Journal of Laws 2023, item 1280, 1429 and 1834); soldier within the meaning of Article 2 point 39 of the Act of 11 March 2022 on the defence of the Homeland (Journal of Laws of 2024 item 248 and 834). The Reporting Party is also the natural person referred to above in the case of reporting or publicly disclosing information about a violation of the law obtained in a work-related context before entering into an employment relationship or other legal relationship constituting the basis for the provision of work or services or the performance of a function in or for a legal entity, or the performance of service in a legal entity, or after their termination.

2.3. **Report –** providing the Company with written information about a violation of the law.

2.4. **External Report –** providing information about a violation of the law to the Commissioner for Human Rights or a public authority orally or in writing.

2.5. **Act –** Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws, item 928).

2.6. **Reports Coordinator reports** – a person within the organizational structure of the Company authorized to receive reports and take follow-up actions, including verification of the report, further communication with the Reporting Party, in particular requesting additional information and providing feedback.

2.7. Retaliatory **actions** – 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 may violate the rights of the Reporting Party or causes or may cause unjustified damage to the whistleblower, including unfounded initiation of proceedings against the Reporting Party.

2.8. **Person related to the Reporting Party** – a natural person who may experience retaliatory action, including a colleague or the closest person to a whistleblower within the meaning of Article 115 § 11 of the Act of 6 June 1997 – Penal Code (Journal of Laws of 2024 item 17). The closest person is a spouse, ascendant, descendant, sibling, relative by marriage in the same line or degree, a person in an adoptive relationship and his or her spouse, as well as a person living in cohabitation.

2.9. **A person helping to make a report** – a natural person who assists the Reporting Party in making a report or public disclosure in a work-related context and whose assistance should not be disclosed.

3. Subject Matter of the Report

3.1. The Reporting Party may provide the Company with information concerning a violation of the law, including information containing a reasonable suspicion regarding an actual or potential violation of the law that has occurred or is likely to occur in the Company in which the Reporting Party participated in the recruitment process or other negotiations preceding the conclusion of a contract, works or worked, or in another legal entity with which the Reporting Party maintains or maintained contact in a work-related context, or information concerning an attempt to conceal such a violation of the law.

3.2. The report may concern actions or omissions that are unlawful or intended to circumvent the law in the following areas:

3.2.1. corruption,

3.2.2. public procurement,

3.2.3. financial services, products and markets,

3.2.4. counteracting money laundering and terrorism financing,

3.2.5. product safety and compliance,

3.2.6. transport safety,

3.2.7. environmental protection,
3.2.8. radiological protection and nuclear safety,
3.2.9. food and feed safety,
3.2.10. animal health and welfare,
3.2.11. public health,
3.2.12. consumer protection,
3.2.13. protection of privacy and personal data,
3.2.14. security of networks and IT systems,
3.2.15. financial interests of the State Treasury of the Republic of Poland, local government units and the European Union,
3.2.16. the European Union internal market, including public law rules on competition and state aid and corporate taxation,
3.2.17. constitutional freedoms and rights of man and citizen - occurring in relations of an individual with public authorities and not related to the areas indicated in points 3.2.1–3.2.16.

4. The Method of Submitting Internal Reports

4.1. The Reporting Party may provide information about a violation of the law by submitting a non-anonymous report, ensuring the possibility of identifying the Reporting Party.
4.2. Reports may only be made in writing: in paper or electronic form.
4.3. The following methods of submitting reports (hereinafter referred to as "reporting channels") are available:
4.3.1. via the dedicated email box at whistleblowing@sescom.eu,
4.3.2. by registered mail to the following address: Sescom S.A., Aleja Grunwaldzka 82, 80-244 Gdańsk, with the note "Internal Report" on the envelope.
4.4. Reporting channels are managed by the Reports Coordinator and their deputy.
4.5. Internal reports might be submitted in Polish or English.
4.6. The internal report should include in particular:
4.6.1. name and surname of the Reporting Party and contact details, i.e. mailing address or e-mail address,
4.6.2. a detailed description of the event and an indication of what the violation of the law is or may be,
4.6.3. indication of the date on which the violation occurred or the date on which information about the violation was obtained,
4.6.4. indication of the place where the violation of the law occurred,
4.6.5. identification of the entity concerned by the violation of the law,
4.6.6. indication of the Reporting Party's connection with the described facts concerning the violation of the law.
4.6.7. indication of evidence confirming the violation of the law, in particular documents, e-mail communications, indication of personal data of witnesses to the event and their contact details,
4.6.8. indication of whether the violation has been previously reported to other organizations or entities. In such a case, it should be clearly stated which organisations or entities were informed of the breach and whether any actions or interventions were taken in response to those reports. If such actions were taken, the Reporting Party should also indicate the results of these actions.
4.7. Reports submitted in a manner other than that specified in points 4.3 and 4.6 will not be considered.

4.8. The Reporting Party who makes a report knowing that no violation has occurred shall be subject to a fine, the penalty of restriction of liberty or imprisonment for up to 2 years in accordance with Article 57 of the Act.

5. Receiving Internal Reports

5.1. The entity responsible for receiving internal reports and exercising overall supervision over their receipt is the person designated in the position of: Head of the Controlling Office (hereinafter referred to as: **"Reports Coordinator").**

5.2. In the absence of the Reports Coordinator, the applications are accepted by his deputy appointed by the Management Board of the Company.

5.3. Before admitting the persons indicated in point 5.1 and 5.2 to the case, each of them is obliged to sign the following documents:

5.3.1. a declaration of impartiality, a template of which is attached as **Annex 1** to this Procedure,

5.3.2. acknowledgement form for this Procedure, the template of which is attached as **Annex 2** to this Procedure,

5.3.3. a statement on maintaining the confidentiality of information obtained during the receipt of internal reports and further proceedings, the template of which is attached as **Annex 3** to this Procedure,

5.3.4. authorization to process personal data, the template of which is attached as **Annex 4** to this Procedure.

5.4. Reports Coordinator and their Deputy are required to keep confidential all information contained in the Report, except for situations in which disclosure is required by law.

5.5. Reports Coordinator will, to the extent possible, confirm the receipt of the Report within 7 days of its receipt, unless the Reporting Party has not provided a contact address to which confirmation should be sent.

5.6. Reports Coordinator may refrain from considering a Report if its subject matter and the facts cited are identical to those of a previous Report submitted by the same or another Reporting Party, and the new Report does not contain any significant additional information concerning the violation. In such a case, the report will be left without consideration and the Reporting Party will be informed thereof without giving any reason.

6. Actions Taken after Receiving the Report – Initial Verification of the Report

6.1. Reports Coordinator or his deputy are obliged to carry out the initial verification of the Report within 15 days from the date of confirmation of receipt of the Report.

6.2. Initial verification of the Report includes:

6.2.1. determining whether the Report concerns at least one violation of the law described in point 3.2 of this Procedure,

6.2.2. determining whether the Report was made by a whistleblower within the meaning of the provisions of the Act,

6.2.3. checking whether the Report contains the information necessary for its consideration,

6.2.4. assessment of the credibility of the Report,

6.2.5. conducting a preliminary analysis of the reported facts and evidence to determine whether there are grounds for initiating further investigative proceedings.

6.3. As part of the initial verification of the Report, if possible, the Reports Coordinator or his deputy may ask the Applicant for additional explanations, unless the Reporting Party failed to provide a contact address.

6.4. The Reporting Party is obliged to respond to clarifying questions as soon as possible. If no response is received within 5 days of receiving the message, the Coordinator will make an appropriate decision based on the facts and evidence available to date.

6.5. Once the initial verification is complete, the Reports Coordinator or their deputy decides on:

6.5.1. leaving the case without further consideration – if the Report proves to be unfounded, incomplete or if it is not possible to obtain the information necessary to conduct further proceedings,

6.5.2. conducting investigative proceedings – if the Report is deemed justified or requires further analysis.

6.6. Reports Coordinator is obliged to inform the Reporting Party of the decision to leave the Report without further consideration, providing a justification for this decision.

7. Investigative Proceedings

7.1. Reports Coordinator shall independently conduct the investigative proceedings within 2 months from the date of the decision referred to in point 6.5.2.

7.2. If the circumstances of the Report require it, the Reports Coordinator has the right to appoint an Investigation Team, which may consist of a maximum of 3 people (hereinafter referred to as "Investigation Team Members"). Investigation Team Members should have appropriate knowledge of the subject of the Report, which will enable them to conduct the investigative proceedings.

7.3. Investigation Team Members cannot be persons in the case of whom there is a risk of violating the principles of impartiality and objectivity in relation to the violation in question; in particular, a member cannot be the direct superior of the Reporting Party or the Management Board of the Company.

7.4. In the event of the appointment of an Investigation Team, the Reports Coordinator acts as the team leader.

7.5. Before being admitted to the investigative proceedings, a Team Member should sign a declaration of confidentiality regarding all information obtained in connection with the proceedings, a declaration of impartiality, an acknowledgement of this Procedure and an authorisation to process personal data.

7.6. A Team Member may be excluded from the investigation in the following cases:

7.6.1. long-term absence that prevents active participation in the proceedings,

7.6.2. the occurrence of a conflict of interest that may affect the impartiality and objectivity of the assessment of the Report,

7.6.3. taking actions that are contrary to accepted ethical standards,

7.6.4. breach of confidentiality of information relating to ongoing proceedings.

7.7. Reports Coordinator or the Investigation Team conducts an in-depth analysis of the Report's content, determines the circumstances of the case and formulates recommendations for further follow-up actions. These activities should be carried out in a fair and objective manner, with due diligence.

7.8. Reports Coordinator or the Investigation Team, if possible and the circumstances of the case require it, have the right to take the following actions:

7.8.1. request the Reporting Party to provide additional information or explanations regarding the Report,

7.8.2. contact other persons who may have significant knowledge about the event that is the subject of the Report (in particular those referred to in the Report as witnesses) in order to collect additional evidence or confirm the circumstances.

7.9. If it is determined that the report is unfounded during the investigative proceedings, the Reports Coordinator or the Investigation Team may refrain from further action and close the case, providing appropriate justification.

7.10. If the reported violation is confirmed, the Reports Coordinator or the Investigation Team is obliged to issue recommendations regarding further corrective or preventive actions aimed at eliminating existing violations indicated in the report and implementing measures to prevent similar incidents in the future.

7.11. Corrective or preventive actions may include, in particular:

7.11.1. modifying or implementing new internal procedures to prevent future violations,

7.11.2. implementing additional training and educational programs for employees and persons cooperating with the Company aimed at raising awareness of the identification of risks and prevention of violations,

7.11.3. implementing structural changes and shifting competences to effectively manage areas covered by reports and minimize risk,

7.11.4. taking disciplinary action against the person concerned by the violation,

7.11.5. taking appropriate legal steps, depending on the nature and context of the event, including filing a report of a suspected crime, initiating court or administrative proceedings.

7.12. In the event that the Reports Coordinator or the Investigation Team has reasonable doubts or when the recommended action requires approval by the Company's Management Board, the Reports Coordinator presents a corrective action plan to the Management Board for approval.

7.13. The Company's Management Board conducts a detailed assessment of the presented corrective action plan. Based on the analysis, the Management Board decides to approve, reject or introduce appropriate changes to the plan.

7.14. The investigation ends with the preparation of a final report, which includes a detailed record of the activities carried out. The report should include in particular the following information:

7.14.1. date of receipt of the report,

7.14.2. subject of the report,

7.14.3. list of all evidence collected during the proceedings,

7.14.4. a detailed description of the circumstances of the incident,

7.14.5. assessment of the validity of the report,

7.14.6. recommendations.

7.15. Reports Coordinator or their deputy will provide feedback to the Reporting Party within a period not exceeding 3 months from the date of confirmation of receipt of the Application or – in the event of failure to provide the confirmation referred to in point 5.5 of this Procedure – within 3 months from the expiry of 7 days from the date of submitting the Report, unless the Reporting Party failed to provide a contact address to which feedback should be sent.

8. Internal Reports Register

8.1. The Company maintains a register of internal reports in electronic form.
8.2. An entry in the register of internal reports is made on the basis of the Report.
8.3. Entry into the register includes reports that are not anonymous.
8.4. The internal reporting register includes:
8.4.1. application number,
8.4.2. the subject of the violation of the law,
8.4.3. personal data of the Reporting Party and the person concerned by the report, necessary to identify these persons,
8.4.4. contact address of the Reporting Party,
8.4.5. date of the report,
8.4.6. information about follow-up actions taken,
8.4.7. date of closing of the case.
8.5. The register of internal reports is kept according to the template attached as **Appendix 5** to this Procedure in electronic form.
8.6. The register of internal reports is kept in a manner that guarantees the confidentiality of the information contained therein.
8.7. Reports Coordinator or their deputy makes entries in the register in a reliable manner, reflecting the actual course of actions taken in connection with the accepted Report.
8.8. Access to the Internal Reports Register is only available to the Reports Coordinator and the designated deputy.
8.9. When justified, law enforcement may also access the Register of internal reports in connection with activities carried out under generally applicable law.
8.10. Personal data and other information in the Reports Register are retained for a period of 3 years after the end of the calendar year in which the follow-up action was completed or after the proceedings initiated by such action were completed.
8.11. The Company is the controller of personal data collected in the internal Report register.

9. Personal Data Protection

9.1. The personal data of the Reporting Party, the person concerned by the report, witnesses and other persons associated with the Reporting Party are kept confidential and are not made available to other employees or third parties, with the exception of persons to whom the data must be made available in order to conduct explanatory activities related to the Report or other activities required by separate regulations.
9.2. With regard to the Reporting Party, the information obligation is fulfilled in accordance with Article 13 GDPR upon first contact with that person. Data Privacy Notice constitutes **Annex 6** to this Procedure.
9.3. Information obligation under Article 14 GDPR with regard to the person concerned by the Report and other third parties whose personal data were provided to the organization by the Reporting Party in the Report is met, with the exception of Article 14 section 2 point f) GDPR, within the period specified in Article 14 section 3 of the GDPR. Data Privacy Notice for persons concerned by the Report and other third parties constitutes **Annex 7** to this Procedure.
9.4. The provisions of Article 14 section 2 point f) GDPR shall apply if the Reporting Party does not meet the conditions specified in Article 6 of the Act or has expressly consented to the disclosure of his or her identity.

9.5. The provisions of Article 15 section 1 point g) GDPR regarding the disclosure of the source of personal data shall apply if the Reporting Party does not meet the conditions specified in Article 6 of the Act or has expressly consented to such transfer.
9.6. Maintaining confidentiality is intended to ensure the safety of the Reporting Party and to minimize the risk of retaliatory or repressive actions. The Reporting Party who has submitted a Report and whose personal data have been disclosed in an unauthorised manner should immediately notify the Data Protection Officer about the situation, who is obliged to take actions to protect the Reporting Party's data.
9.7. The identity of the Reporting Party, as well as any information enabling their identification, will not be disclosed to any persons concerned by the Report (e.g. employer, employee, collaborator, supplier, customer to whom the Report concerns), third parties or other employees and collaborators of the Company, unless with the express consent of the Reporting Party or in the event that the Reporting Party does not meet the conditions specified in Article 6 of the Act.
9.8. The identity of the Reporting Party, as well as other information enabling their identification, may be disclosed only if such disclosure is a necessary and proportionate obligation resulting from generally applicable provisions of the law in the context of proceedings conducted by national authorities. The identity of the entities concerned by the Report, persons assisting in making the report and persons associated with the reporting party are subject to confidentiality requirements to the same extent as the identity of the Reporting Party.
9.9. Personal data, except for the Reporting Party's data, processed in connection with the acceptance of the Report are stored by the Company for no longer than 3 years from the date of acceptance of the Application.
9.10. The above point does not apply when the documents related to the Report constitute part of the files of preparatory proceedings or court or administrative court cases.

10. Protection against Retaliatory Actions

10.1. The Company takes steps to protect the Reporting Party against retaliatory actions, including attempts or threats of such actions.
10.2. Protection also covers persons assisting in submitting a Report and persons associated with the Reporting Party.
10.3. If the work has been, is or will be performed on the basis of an employment relationship, the Reporting Party may not be subject to retaliatory action, in particular by:
10.3.1. refusal to enter into an employment relationship,
10.3.2. notice of termination or termination without notice of the employment relationship,
10.3.3. failure to conclude a fixed-term employment contract or an employment contract for an indefinite period following the termination of a trial period employment contract, failure to conclude another fixed-term employment contract or failure to conclude an employment contract for an indefinite period following the termination of a fixed-term employment contract – if the whistleblower had a justified expectation that such a contract would be concluded with him,
10.3.4. reducing the amount of remuneration for work,
10.3.5. withholding promotion or being passed over for promotion,
10.3.6. omission when granting work-related benefits other than remuneration or reducing the amount of such benefits,
10.3.7. transfer to a lower job position,

10.3.8. suspension from the performance of employment or service duties,
10.3.9. transferring the current whistleblower duties to another employee,
10.3.10. an unfavourable change in the place of work or working time schedule,
10.3.11. negative evaluation of work results or negative opinion about work,
10.3.12. the imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature,
10.3.13. coercion, intimidation or exclusion,
10.3.14. mobbing,
10.3.15. discrimination,
10.3.16. unfavourable or unfair treatment,
10.3.17. suspension of participation or omission when selecting for participation in training to improve professional qualifications,
10.3.18. unjustified referral for medical examinations, including psychiatric examinations, unless separate provisions provide for the possibility of referring an employee for such examinations,
10.3.19. action aimed at making it more difficult to find future work in a given sector or industry on the basis of an informal or formal sectoral or industry agreement,
10.3.20. causing financial loss, including economic loss, or loss of income,
10.3.21. causing other non-material damage, including infringement of personal rights, in particular the good name of the Reporting Party.

11. External Reports

11.1. The reporting party may make an external report without first making an internal report.
11.2. An external report may be made to the Commissioner for Human Rights or the appropriate authority for a given category of violation of the law.

12. Final Resolutions

12.1. The Management Board of the Company is responsible for the implementation and effectiveness of this Procedure.
12.2. The internal reporting procedure will be reviewed periodically. The Company reserves the right to make changes to the Procedure. These changes may be introduced as needed, in particular resulting from changes in legal provisions.
12.3. The procedure comes into force 7 days after the date of announcement on the internal Intranet.
12.4. On the date of entry into force, the Procedure will replace the solutions for reporting violations in relation to Sescom S.A. adopted by the Company in the *Ethical Conduct Policy of Sescom S.A. and the Sescom S.A. Capital Group* in section VI "Reporting abuse and protection of reporting parties" adopted by the resolution of the Management Board of Sescom S.A. of 10 January 2020.

13. Annexes

Annex 1 – Declaration of Impartiality,
Annex 2 – Acknowledgement of the Procedure,
Annex 3 – Confidentiality Statement,
Annex 4 – Authorization to Process Personal Data,

Annex 5 – Register of Internal Reports,
Annex 6 – Data Privacy Notice for the Reporting Party,
Annex 7 – Data Privacy Notice for the Person Concerned by the Report and Other Third Parties.

Annex 1 – Declaration of impartiality

Gdansk, on ……

DECLARATION OF IMPARTIALITY

I, the undersigned, hereby declare that in connection with the performance of my duties of receiving internal reports or conducting investigative proceedings in accordance with the **Internal Reporting Procedure** in force at Sescom S.A. there are no circumstances, nor are they known to me, that might give rise to doubts as to my impartiality and objectivity.

At the same time, I declare that in the event of disclosure or obtaining information about any circumstance that could give rise to justified doubts as to my impartiality or objectivity in relation to the accepted report or the conducted investigative proceedings, I undertake to immediately inform the Management Board of the Company of this fact and to exclude myself from further participation in the acceptance of the report, the investigative proceedings and in taking any follow-up actions.

legible signature

Annex 2 – Acknowledgement of the Procedure

Gdansk, on ……..

ACKNOWLEDGEMENT OF THE PROCEDURE

I, the undersigned, hereby declare that I have read the "Internal Reporting Procedure" in force at Sescom S.A., understand its content, accept its application and undertake to comply with the principles contained therein.

legible signature

Annex 3 – Confidentiality statement

CONFIDENTIALITY STATEMENT

1. I, the undersigned, hereby undertake to keep confidential the information obtained in connection with the receipt and verification of internal reports or participation in investigations and taking follow-up actions/participating[1] in investigative proceedings and taking follow-up actions in cases concerning reports of irregularities conducted by Sescom S.A. carried out as part of the Internal Reporting Procedure.
2. "Confidential Information" shall be understood in particular as any information on the basis of which it is possible to directly or indirectly identify the identity of the person reporting the violation (hereinafter referred to as the "Reporting Party"), the person concerned by the report and the third party indicated in the report, the person assisting in making the report or the person associated with the Reporting Party, as well as the content of the report of the violation and any explanations provided during the investigative proceedings.
3. Therefore, I undertake to:

a) use the above information only to the extent necessary to receive and verify internal reports or participate in investigations and take follow-up actions/participating[2] in investigative proceedings and taking follow-up actions,

b) not to make available, transfer or disclose Confidential Information to any person except where a court requires such disclosure or where there is a statutory obligation to do so,

c) adequately protect the above information against access by unauthorized persons, including unauthorized disclosure, disclosure, copying, use, modification, damage or loss.

4. The obligation to keep Confidential Information confidential is valid for an indefinite period of time, even after the performance of the entrusted activities and after the termination of the employment relationship or other legal relationship under which the activities were performed.
5. Conduct contrary to the above obligations may constitute a violation of criminal provisions, including Article 56 of the Act of 14 June 2024 on the protection of whistleblowers (Journal of Laws, item 928) and may also give rise to civil liability for damages.

place and date legible signature

[1] Cross out where inapplicable. Reports Coordinator and their deputy should commit to choosing the first option. [signature of the authorized person]

[2] Cross out if inapplicable. The members of the Investigation Team should commit to choosing the second option.

Annex 4 – Authorization to process personal data

AUTHORIZATION
TO PROCESS PERSONAL DATA

As of ……., I authorize:

Mrs./Mr.: ……

job position or function: …….

to process personal data as part of the processing of personal data of whistleblowers for purposes related to the performance of duties resulting from the position entrusted or the function performed, in accordance with the Controller's instructions and to the extent necessary and required to fulfil the legal obligations incumbent on the Controller.

in the form:
a) Electronic (Electronic box): Yes/ ~~No~~ *
b) Traditional (paper documents): Yes/ ~~No~~ *

The authorisation ceases to apply upon termination of the employment relationship/contract or withdrawal of authorisation to process personal data. The authorisation is issued for the period of holding the position or function in question or for the period of written revocation of this authorisation.

This authorization obliges you to process personal data in accordance with the authorization granted, the provisions on personal data protection and internal regulations issued by the Controller in this respect, including the obligation to keep personal data and methods of securing them confidential, for an unlimited time, as well as to report any breach or threat to personal data security.

[signature of the authorizing person]

Annex 5 – Internal Reports Register

INTERNAL REPORTS REGISTER

Report number	Subject of violation	Personal data of the reporting party necessary for identification	Contact address of the reporting party	Date of internal report	Information on follow-up actions taken	Case-closed date
1.						
2.						
3.						
4.						

Annex 6 – Data Privacy Notice

DATA PRIVACY NOTICE FOR THE REPORTING PARTY IN CONNECTION WITH THE SUBMITTED REPORT

In accordance with article 13 of 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 (hereinafter referred to as GDPR), the Data Controller informs:

1. **Data Controller** – the Controller, i.e. the entity deciding which personal data will be processed, for what purpose and in what manner, is Sescom S.A., ul. Grunwaldzka 82, 80-244 Gdansk, email: info@sescom.eu .
2. **Data Protection Officer** – in all matters relating to the protection of personal data, you have the right to contact our data protection officer at the following e-mail address: iod@sescom.eu .
3. **Purpose of processing** – personal data will be processed for the purpose of enabling the reporting of violations of the law, in accordance with the Act mentioned below, and the performance of obligations related to the report.
4. **The basis for processing personal data**

1) article 6 section 1 point c) GDPR – fulfilment of a legal obligation, in connection with the provisions of the Act of 14 June 2024 on the protection of whistleblowers in order to carry out tasks related to the handling of internal reports (in particular: receiving and verifying the report, keeping a register of internal reports, conducting correspondence with the reporting party, archiving the case),

2) article 9 section 2 point g) GDPR – when data processing is necessary for reasons related to important public interest in connection with the provisions of the Act on the Protection of Whistleblowers, if personal data of special categories are included in the internal report,

3) article 6 section 1 point a) GDPR – consent of the Reporting Party to disclose their identity, which will allow us to disclose the identity of, among others, the person to whom the report relates.

5. **Obligation to provide data** – providing personal data resulting from legal provisions is obligatory. Consent is completely voluntary and may be withdrawn at any time.
6. **Data storage period** – personal data will be stored for a period of 3 years after the end of the calendar year in which the follow-up actions were completed, or after the completion of the proceedings initiated by these actions, i.e. for the period specified in the Act on the Protection of Whistleblowers.
7. **Data recipients** – personal data will be made available only to entities authorized to process them under legal provisions or signed agreements. Personal data will be made available to separate controllers, i.e. competent authorities for follow-up action.
8. **Personal rights** – you have the right to request access to your personal data, obtain a copy of your personal data, correct your data, limit their processing and the right to lodge a complaint with the President of the Personal Data Protection Office (ul. Stawki 2, 00-193 Warsaw, e-mail: kancelaria@uodo.gov.pl) . Furthermore, with respect to data processed on the basis of consent, you have the right to withdraw this consent at any time. Withdrawal of consent does not affect the lawfulness of the processing which was carried out on the basis of consent before its withdrawal. You can withdraw your consent by sending a request to our e-mail or postal address. The consequence of withdrawing the consent will be our inability to process this data.

Annex 7 – Data Privacy Notice for the person concerned by the Report and other third parties

DATA PRIVACY NOTICE FOR THE PERSON CONCERNED BY THE REPORT AND OTHER THIRD PARTIES PROVIDED BY THE REPORTING PARTY IN CONNECTION WITH THE SUBMITTED REPORT

In accordance with article 14 of 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 (hereinafter referred to as GDPR), the Data Controller informs:

1. **Data Controller** – the Controller, i.e. the entity deciding which personal data will be processed, for what purpose and in what manner, is Sescom S.A., ul. Grunwaldzka 82, 80-244 Gdansk, email: info@sescom.eu .
2. **Data Protection Officer** – in all matters relating to the protection of personal data, you have the right to contact our data protection officer at the following e-mail address: iod@sescom.eu .
3. **Purpose of processing** – personal data will be processed for the purpose of enabling the reporting of violations of the law, in accordance with the Act mentioned below, and the performance of obligations related to the report.
4. **The basis for processing personal data**

1) article 6 section 1 point c) GDPR – fulfilment of a legal obligation, in connection with the provisions of the Act of 14 June 2024. on the protection of whistleblowers in order to carry out tasks related to the handling of internal reports (in particular: receiving and verifying the report, keeping a register of internal reports, conducting correspondence with the reporting party, archiving the case),

2) article 9 section 2 point g) GDPR – when data processing is necessary for reasons related to important public interest in connection with the provisions of the Whistleblower Protection Act, if personal data of special categories are included in the internal report.

5. **Obligation to provide data** – providing personal data resulting from legal provisions is obligatory. Consent is completely voluntary and may be withdrawn at any time.
6. **Data storage period** – personal data will be stored for a period of 3 years after the end of the calendar year in which the follow-up actions were completed, or after the completion of the proceedings initiated by these actions, i.e. for the period specified in the Act on the Protection of Whistleblowers. Personal data may be processed for a longer period than indicated above in situations where documents related to an internal report form part of preparatory proceedings or court or administrative court case files.
7. **Data recipients** – personal data will be made available only to entities authorized to process them under legal provisions or signed agreements. Personal data will be made available to separate controllers, i.e. competent authorities for follow-up action.
8. **Personal rights** – you have the right to request access to your personal data, obtain a copy of your personal data, rectify your data, limit their processing and the right to file a complaint with the President of the Personal Data Protection Office (ul. Stawki 2, 00-193 Warsaw, e-mail: kancelaria@uodo.gov.pl) .
9. **Data Source** – data source in accordance with Article 8 section 5 of the Act on the Protection of Whistleblowers is not public, unless the whistleblower fails to meet the conditions specified in Article 6 above the Act or expressly consents to the disclosure of his or her identity or the transfer of data.
10. **Data Categories** – data provided by the whistleblower in an internal report may include identifying data: name and surname, position, place of work, description of the violation.