§1.

Preliminary provisions.

1. Pursuant to article 25, sections 1 and 2 of the Act of 14 June 2024 on the Protection of Whistleblowers (Journal of Laws of 2024, item 928), the internal reporting procedure is established in the Luma Group, which defines the rules for reporting breaches of the law, taking follow-up actions, and protecting reporting persons (whistleblowers), hereinafter referred to as '**the procedure**'.
2. The purpose of the procedure is:
   - creation of a comprehensive regulation for the issue of disclosing cases of irregularities and protecting reporting persons (whistleblowers),
   - ensuring the lawful functioning of the organisation,
   - preventing and combating any irregularities related to the operation of the organisation,
   - safeguarding the interests of legal entities within the Luma Group, regardless of obligations stemming from national or European law,
   - creating a culture of responsibility within the organisation and regulating the process of reporting and investigating reported irregularities,
   - improving public perception of the actions of individuals reporting irregularities, who are often viewed as morally questionable (denouncing),
   - protecting persons reporting cases of irregularities,
   - promoting a sense of civic responsibility.
3. Each legal entity belonging to the Luma Group guarantees that the internal reporting procedure and the related processing of personal data during the submission of reports prevent unauthorised persons from accessing the information covered by the report and ensure the confidentiality of the identity of the whistleblower, the person concerned, and any third party mentioned in the report. The confidentiality protection applies to information that may directly or indirectly identify the identity of such individuals.
4. Each person performing work on the basis of an employment relationship or other legal relationship constituting the basis for the provision of work, services, or the performance of functions or service, is obliged to familiarise themselves with the content of the internal reporting procedure and to comply with it.
5. A person applying for employment on the basis of an employment relationship or other legal relationship constituting the basis for the provision of work, services, or the performance of functions or service must be informed about the internal reporting procedure at the commencement of recruitment or negotiations preceding the conclusion of the contract.
6. Wherever in the Procedure reference is made to:

   1) **act** - this is to be understood as the act of 14 June 2024, on the Protection of Whistleblowers**;**
   2) **whistleblower** – this is to be understood as:
      a. An individual who reports or publicly discloses information about a breach of the law obtained in a work-related context, including an employee, a temporary worker, a person performing work on a basis other than an employment relationship, including under a civil law contract, an entrepreneur, a commercial proxy, a shareholder or partner, a member of the governing body of a legal entity or an organisational unit without legal personality,

a person performing work under the supervision and direction of a contractor, subcontractor, or supplier, an intern, a volunteer, or a trainee;

b. an individual referred to in point a., in the case of reporting or publicly disclosing information about a breach of the law obtained in a work-related context before establishing an employment relationship or other legal relationship constituting the basis for providing work or services, or performing a function in a legal entity or on behalf of that entity, or performing service in a legal entity, or after the termination of such a relationship.

3) **Group Luma** – this refers to a group of private entities belonging to a capital group as defined in Article 4, point 14 of the Act of 16 February 2007 on Anti-Trust and Consumer Protection (Journal of Laws of 2024 item 594) i.e., Luma Services Sp. z o.o., Re Alloys Sp. z o.o. Odlewnia Kutno Sp. z o.o., Zakłady Metalowe „Postęp" S.A., Saga Poland Sp. .z o.o. for which a shared internal reporting procedure can be established, provided that the actions performed are in compliance with the law;
4) **legal entity** - this is understood as a private entity belonging to the Luma Group;
internal reporting - this is understood as the submission of information regarding a breach of law to a legal entity in writing, via email.
5) **external reporting** – this is understood as the oral or written submission of information to the Ombudsman or a public authority regarding a breach of law;
6) ***follow-up*** – this is understood as an action taken by an authorised entity to assess the truthfulness of the information contained in the report and to prevent the breach of law that is the subject of the report, particularly through an investigation, initiation of an audit or administrative procedure, filing of charges, action taken to recover financial resources, or the closure of the procedure carried out as part of the internal procedure for reporting breaches of law and taking follow-up actions.
7) ***retaliation*** – this is understood as any direct or indirect action or omission in a work-related context that is caused by a report or public disclosure and that infringes or may infringe upon the rights of the whistleblower, or causes or may cause unjustified harm to the whistleblower, including the baseless initiation of proceedings against the whistleblower;
8) ***information on a breach of the law*** – this is understood as information, including a reasonable suspicion, regarding an actual or potential breach of the law that has occurred or is likely to occur in a legal entity in which the whistleblower participated in the recruitment process or other negotiations preceding the conclusion of an agreement, is employed or was employed, or in another legal entity with which the whistleblower maintains or maintained contact in a work-related context, or information regarding an attempt to conceal such a breach of the law.
9) ***feedback*** – this is understood as information provided to the whistleblower regarding the planned or undertaken follow-up measures and the reasons for such actions;
10) **work-related context** - this is understood as past, present, or future activities related to the performance of work based on an employment relationship or another legal relationship that serves as the basis for providing work or services or performing functions in a legal entity or on behalf of that entity, or serving in a legal entity, within which information about a breach of the law was obtained and there is a possibility of experiencing retaliatory measures;

11) **public authority** - this is understood as the supreme and central government administration bodies, local government administration bodies, bodies of local government units, other state bodies, and other entities performing public administration tasks by law, competent to undertake follow-up actions in the areas specified in Article 3(1) of the Act;
12) **person concerned** - this is understood as a natural person, legal entity, or organisational unit without legal personality, granted legal capacity by the law, identified in the report or public disclosure as a person who committed a breach of law, or as a person associated with the individual who committed the breach of law;
13) **facilitator** - this is understood as a natural person who assists a reporting person in the reporting process or public disclosure in a work-related context, and whose assistance should be confidential;
14) **person associated with the whistleblower** - this is understood as a natural person who may experience retaliatory measures, including a co-worker or a person close to the whistleblower, as defined in Article 115 § 11 of the Act of 6 June 1997 - the Criminal Code (Journal of Laws of 2024 item 17),
15) public disclosure - this is understood as the provision of information regarding a breach of law to the public;
16) **legal proceeding** - this is understood as a proceeding pending based on generally applicable law, in particular criminal, civil, administrative, disciplinary proceedings, or proceedings concerning a breach of public finance discipline, or a proceeding conducted based on internal regulations adopted to implement generally applicable law, particularly anti-mobbing regulations;
17) **GDPR** - this is understood as the Regulation (EU) No. 2016/679 of the European Parliament and 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/WE (General Data Protection Regulation) (Official Journal of UE of 2016, no.1481, as amended).

§2.
Internal reporting

1. The entity authorised by individual private entities within the Luma Group to receive reports is the Audit Department of Luma Services Sp. z o.o. (hereinafter: the “Audit Department”) or external entity. A draft of the authorisation constitutes the appendix No. 1 hereto.
2. A report can be submitted via email to the following address: sygnalista@lumaservices.eu
3. In the event that the report of a breach pertains to the Audit Department, the report should be submitted via email to the following address zarzad@lumaservices.eu.
4. The report should primarily include:
   a) reporting date;
   b) reporting person’s details, i.e., first name, last name, contact email address, and indication of the work-related context;
   c) job position;
   d) person concerned;
   e) details of the individuals who committed the breach of law, i.e., first name, last name, position, and workplace;
   f) a description of the irregularities and the dates on which they occurred.
5. The report may additionally be documented with collected evidence and a list of witnesses.

6. A draft for the irregularity/breach report form constitutes appendix no. 2 to the procedure.
7. Anonymous reports will not be processed.
8. The subject of the report may include breaches of law in the form of actions or omissions that are unlawful or aimed at circumventing the law concerning:
   1) corruption;
   2) public procurement;
   3) financial services, products and markets;
   4) prevention of money laundering and terrorist financing;
   5) product safety and compliance;
   6) transport safety;
   7) environmental protection;
   8) public health;
   9) consumer protection;
   10) protection of privacy and personal data;
   11) security of network and information systems;
   12) the financial interests of the State Treasury of the Republic of Poland, local government units, and the European Union;
   13) the internal market of the European Union, including public law rules on competition and state aid, as well as corporate taxation;
   14) breaching applicable regulations, procedures, customs, and ethical standards established by the legal entity within the Luma Group.
9. The procedure does not cover the reporting of information that is subject to:
   a) provisions on the protection of classified information and other information that cannot be disclosed under generally applicable law for reasons of public safety;
   b) professional secrecy of medical and legal professions;
   c) the secrecy of judicial deliberations;
   d) criminal proceedings, in terms of the confidentiality of preparatory proceedings and the secrecy of court hearings conducted in closed sessions.

§3.
Report Receipt Acknowledgement

1. The entity authorised to receive internal reporting, upon receiving an internal report, is obligated to confirm receipt of the report to the reporting person within 7 days from the date of the receipt. A draft for the confirmation of receipt is provided in Appendix no. 3 to the procedure.
2. The entity authorised to receive internal reports is exempt from the obligation mentioned in paragraph 1 above if the reporting person has not provided contact details (email address) to which the confirmation of receipt should be sent.

§4.
Obligation to take follow-up actions

1. The individuals authorised to take follow-up actions are authorised persons from the Legal Department, Accounting Department, and Audit Department of Luma Services Sp. z o.o. A draft of the authorisation constitutes the appendix No. 1 hereto.

2. The entity authorised to take follow-up actions is obligated to act with due diligence in carrying out these actions.
3. The entity authorised to take follow-up actions is required to provide feedback to the reporting person within a maximum of 3 months from the report receipt acknowledgement, as referred to in §2 above, or if no acknowledgement has been provided, within 3 months from the expiration of 7 days from the date of the report.
4. The entity authorised to receive internal reports is exempt from the obligation mentioned in paragraph 3 above if the reporting person has not provided contact details (email address) to which the feedback should be sent.
5. After conducting the investigation, the entity authorised to take follow-up actions issues recommendations for appropriate corrective measures and recommendations aimed at eliminating and preventing the recurrence of identical or similar breaches to those described in the report in the future.

§5.

Internal reporting

1. The whistleblower may make an external reporting without first submitting an internal reporting.
2. The external reporting is received by the Ombudsman or a public authority. The Ombudsman establishes the procedure for receiving external reports, which specifically outlines the process for handling anonymously reported legal breaches.
3. The Ombudsman and the public authority are separate controllers with regard to the personal data provided in the external reporting received by these authorities.
4. The preliminary verification of an external reporting by the Ombudsman involves determining whether the report concerns information about a breach of law and identifying the public authority responsible for taking follow-up actions.
5. If the external reporting concerns a breach of law, the Ombudsman immediately, but no later than 14 days from the date of the report, forwards the report to the public authority responsible for taking follow-up actions.
6. The Ombudsman informs the whistleblower about the forwarding of the external reporting. The information includes at least the identification of the public authority to which the external report was forwarded and the date of forwarding.
7. The Ombudsman refrains from forwarding the external report if it does not concern information about a breach of law.
8. The Ombudsman informs the whistleblower about the decision not to forward the external report, providing the findings from the preliminary verification of the report.
9. When refraining from forwarding the external report, the Ombudsman may inform the whistleblower that the information included in the report may be considered under separate legal provisions, particularly as the subject of a civil lawsuit, a notification of suspected criminal activity, a complaint to an administrative court, a complaint, request, or petition, or it may be referred to the appropriate authorities for consideration under another procedure. Notifying the whistleblower does not affect, in particular, the admissibility of a later legal remedy, the running of deadlines, or the content of the decision or the manner of concluding the proceedings. The information provided to the whistleblower contains guidance in this regard.

§6.

Public disclosure

1. A Whistleblower making a public disclosure is entitled to protection if they make:
   1) an internal reporting, followed by an external reporting, and the legal entity, and then the public authority, do not take any appropriate follow-up actions or provide feedback to the whistleblower within the timeframe for providing feedback as set out in the internal procedure and subsequently in the external procedure of the public authority or
   2) an external reporting and the public authority within the time limit for providing feedback specified in its external procedure, does not take any appropriate follow-up actions or fails to provide feedback to the whistleblower,

   - unless the whistleblower has not provided a contact address to which such information should be sent.

2. A whistleblower making a public disclosure is entitled to protection if they have reasonable grounds to believe that:
   1) the breach may pose a direct or obvious threat to the public interest, particularly if there is a risk of irreversible harm, or
   2) making an external reporting would expose the whistleblower to retaliatory measures, or
   3) there is little likelihood of effectively addressing the breach of law through external reporting due to specific circumstances of the case, such as the possibility of evidence being concealed or destroyed, the existence of collusion between the public authority and the perpetrator of the breach, or the involvement of the public authority in the breach.
3. When assessing whether follow-up action is appropriate, particular consideration is given to the actions taken to verify the information about the breach, the accuracy of the assessment of the breach, and the adequacy of the measures taken in response to the confirmed breach, including—where appropriate—measures to prevent further breaches, taking into account the severity of the breach.
4. The provisions of paragraphs 1-3 above do not apply if the information about the breach of law is disclosed directly to the press, and in such cases, the Act of 26 January 1984 - Press Law, applies (Journal of Laws of 2018 item 1914),

§7.

Prohibition of retaliatory measures and whistleblower protection measures

1. Retaliatory measures, or attempts or threats to take such measures, cannot be taken against a whistleblower
2. If the work was, is, or will be performed based on an employment relationship, retaliatory measures against the whistleblower are prohibited, particularly in the form of:
   1) refusal to establish an employment relationship;
   2) termination or dismissal of employment without notice;
   3) failure to conclude a fixed-term or permanent employment contract after the expiration of a probationary period, failure to conclude a subsequent fixed-term contract, or failure to conclude a permanent employment contract after the expiration of a fixed-term contract – in cases where the Whistleblower had a legitimate expectation that such a contract would be concluded;
   4) reduction in salary;
   5) withholding or omission in promotions;
   6) omission in granting work-related benefits other than salary, or reduction of such benefits;

7) demotion to a lower position;
8) suspension from performing employee or official duties;
9) transfer of the whistleblower's current duties to another employee;
10) unfavourable changes in the workplace or work schedule;
11) negative performance assessment or employment reference;
12) imposition or administering of disciplinary measures, including financial penalties or similar measures;
13) coercion, intimidation, or exclusion;
14) harassment;
15) discrimination;
16) unfavourable or unfair treatment;
17) withholding or omission in nominating for participation in professional qualification training;
18) unjustified referral to medical examinations, including psychiatric evaluations, unless separate regulations provide for the possibility of referring an employee to such examinations;
19) actions aimed at hindering future employment in the given sector or industry through formal or informal sectoral or industry agreements;
20) causing financial loss, including economic loss or loss of income;
21) causing other non-material harm, including breaches of personal rights, particularly the Whistleblower's good name.

3. Retaliatory measures due to making a report or public disclosure also include attempts or threats to apply any measure specified in paragraph 3.
4. If work or services were, are, or will be performed under a legal relationship other than an employment relationship, which serves as the basis for the provision of work, services, or performance of duties or service, the provisions of this paragraph apply accordingly, provided that the nature of the work or services, or the duties or service performed, does not exclude such actions against the whistleblower.
5. If work or services were, are, or will be performed under a legal relationship other than an employment relationship, the making of a report or public disclosure cannot serve as grounds for retaliatory measures or attempts or threats of retaliatory measures, including in particular:
   1) termination of an agreement to which the whistleblower is a party, especially regarding the sale or delivery of goods or the provision of services, withdrawal from such an agreement, or termination without notice;
   2) imposition of obligations or refusal to grant, restriction, or revocation of rights, in particular licences, permits, or concessions.
6. Protection also extends to a facilitator, as well as a person associated with the whistleblower, and to a legal entity or another organisational unit assisting the whistleblower or associated with them, in particular, one owned by or employing the whistleblower.

§8.
Register of reports

1. Each legal entity within the Luma Group has authorised the Audit Department to maintain the register of internal reports.
2. Entries in the register of internal reports are made based on the internal report.
3. The register of internal reports includes:
   1) report number;

2) subject of the breach of law;
3) personal data of the whistleblower and the person concerned, necessary for the identification of these individuals;
4) contact address of the whistleblower;
5) date of the reporting;
6) information on follow-up actions taken;
7) date of case closure.

4. The controller of the personal data collected in this register is each legal entity within the Luma Group, to the extent that it concerns that particular entity.
5. Personal data and other information in the register of internal reports are stored for a period of 3 years after the end of the calendar year in which follow-up actions were concluded, or after the conclusion of proceedings initiated by those actions.
6. The register of reports is maintained according to the draft provided in appendix no. 4 to the procedure.

§9.
Principles of personal data processing in connection with receiving reports or taking follow-up actions

1. The Whistleblower's personal data, which could reveal their identity, shall not be disclosed to unauthorised persons unless the whistleblower explicitly consents to it.
2. The provision of paragraph 1 does not apply in cases where disclosure is a necessary and proportionate obligation arising from legal provisions in connection with investigative proceedings conducted by public authorities, or preparatory or judicial proceedings conducted by courts, including for the purpose of guaranteeing the right of defence of the person concerned.
3. Before making the disclosure referred to in paragraph 2, the relevant public authority or court shall inform the whistleblower, sending an explanation of the reasons for the disclosure of their personal data in paper or electronic form, unless such notification would jeopardise the investigative, preparatory, or judicial proceedings.
4. The legal entity or public authority, upon receiving the report, processes personal data to the extent necessary for the receipt of the report or for taking any follow-up action. Personal data that are irrelevant to the consideration of the report will not be collected, and if received, it will be promptly deleted. Such data will be deleted within 14 days of determining that it is irrelevant to the case.
5. The provision of Article 14(2)(f) of the GDPR does not apply unless the whistleblower fails to meet the conditions specified in Article 6 of the Act or has given explicit consent to disclose their identity.
6. The provision of Article 15(1)(g) of the GDPR, regarding the disclosure of the source of personal data, does not apply unless the whistleblower fails to meet the conditions specified in Article 6 of the Act or has given explicit consent for such disclosure.
7. Personal data processed in connection with the receipt of the report or follow-up actions, as well as documents related to the report, are stored by the legal entity and the public authority for a period of 3 years after the end of the calendar year in which the external report was forwarded to the relevant public authority for follow-up actions, or follow-up actions were concluded, or after the conclusion of proceedings initiated by those actions.

§10.
Liability for false reports

1. A whistleblower is protected from the moment of making a report or public disclosure, provided that they had reasonable grounds to believe that the information reported or disclosed was true at the time of the report or public disclosure and that it constitutes information about a breach of the law.

2. A person who makes a report without meeting the conditions specified in paragraph 1 above is not entitled to the protection granted to whistleblowers. This means that such a person may be subject to disciplinary action as defined in the provisions of the Labour Code, and such behaviour may also result in the termination of the employment contract without notice. For individuals providing work, services, or delivering goods under a civil law contract, such behaviour may result in the termination of the contract.

3. Whoever makes a report or public disclosure knowing that no breach of the law has occurred shall be subject to a fine, restriction of liberty, or imprisonment for up to 2 years.

§11.
Final provisions

1. In matters not regulated by this procedure, the provisions of the Act of 14 June 2024 on the Protection of Whistleblowers shall apply.
2. The procedure is available on the iHR portal, on the website, and in paper form in the HR department of each legal entity within the Luma Group.

Appendix no. 1 to the procedure for reporting breaches of the law and taking follow-up actions in the Luma Group

Appointment of a person authorised to receive reports from whistleblowers.

Appointment date: ……
Pursuant to article 28(3) and article 25(1)(1) of the Act of 14 June 2024 on the Protection of Whistleblowers, hereby we appoint

…… full name to receive internal reports from whistleblowers making reports in a work-related context within one of the entities of the Luma Group. Reports may only be accepted in accordance with the applicable legal provisions and in compliance with the Internal Procedure.
Email address for receiving reports:
The authorisation period: ……from 25 September 2024 – until revoked……
Note: 1. Whoever, contrary to the provisions of the act, discloses the identity of a whistleblower, a person assisting in making a report, or a person associated with the whistleblower, shall be subject to a fine, restriction of liberty, or imprisonment for up to 1 year. 2. Whoever processes personal data without legal grounds or is not authorised to process such data is subject to a fine, restriction of liberty, or imprisonment for up to two years.
Received on: …… Date and the appointed person's signature
On behalf of the appointers:

Appendix no. 1a to the procedure for reporting breaches of the law and taking follow-up actions in the Luma Group

On .....

AUTHORISATION NO. .....

to process personal data

in IT systems or in paper-based records

Pursuant to article 29 of the Regulation (EU) No. 2016/679 of the European Parliament and 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/WE (General Data Protection Regulation) (Official Journal of the European Union L of 2016, no.119, as amended) hereinafter: GDPR, and article 30(2) of the Whistleblowers protection act,

As of....

I authorise .....

to undertake follow-up actions and to process the personal data of reporting persons, as well as to process the personal data collected in:

1. IT systems (specify the names of systems or programs):
   1) .....,
   2) .....,
2. in paper-based records (specify the names of records):
   1) register of reports
   2) .....,
   3) .....,

in terms of: (V) viewing, (E) entering, (M) modifying, (D) deleting, (A) archiving, (S) sharing with other entities, (N) necessary for performing job duties.

This authorisation does not entitle the holder to grant further authorisations and expires on the date of termination of employment. Additionally, it may be modified or revoked at any time.

Authorised persons are obliged to maintain confidentiality.

Upon signing of this authorisation, authorisation no. ..... granted on .....is hereby revoked.

. . . . . .

(seal and signature of the Personal Data Controller)

Appendix no. 2 to the procedure for reporting breaches of the law and taking follow-up actions in the Luma Group

Irregularity/Breach of Law Report Form

Reporting date: …….
Non-anonymous reporting: Full name - …….. Department/division; position/function - …….. Employee, former employee, or job applicant - ..... Person concerned - ..... Contact details (phone no., e-mail) - ……..
I consent to the disclosure of my personal data: Yes ☐ *No* ☐
Date (time period) and location of the irregularities, or date, location, and source of obtaining information about the irregularities: …… ……..
Content of the report: *(Please provide a detailed description of the situation, event, and circumstances that indicate the occurrence of irregularities)* …… …… ……
Identification of the person or persons to whom the report pertains (*name, position or function, workplace*): …….
Identification of potential witnesses (*if you know any witnesses to the irregularities, provide their names and positions/functions), if you have evidence of the irregularities – provide it and, if possible, attach it to the report*)…… ……..
Identification of potential evidence (*if you have any evidence or information about the irregularity that may be helpful in the review process, provide it and, if possible, attach it to the report*)…… ……
Declaration of the reporting person I hereby declare that by making this report: 1) I am acting in good faith; 2) I have a reasonable belief that the allegations contained in the disclosed information are true; 3) I am not making the disclosure for personal gain; 4) the disclosed information is accurate to the best of my knowledge, and I have disclosed all facts and circumstances known to me concerning the subject of the report; 5) I am familiar with the procedure adopted within the Luma Group for reporting irregularities and the protection of individuals making reports.

…… Date and legible signature of the reporting person (not applicable for anonymous reports)

Appendix no. 3 to the procedure for reporting breaches of the law and taking follow-up actions in the Luma Group

Report Receipt Acknowledgement Form.

Date of receipt of the report: …….
Hereby, I CONFIRM the receipt of the report, which has been registered under case number: …….
Information on processing of personal data: **b) The personal data controller is ……..** **contact: ……** **c) The Controller has assigned the Data Protection Officer who can be contacted via mail to: iod@lumaservices.eu** **d) Purposes of personal data processing are:** **a) initiation of actions aimed at determining whether the reported action or omission constitutes an actual or potential breach of the law** **b) meeting the obligations imposed on the Data Controller by the Protection of Whistleblowers Act** **e) The legal basis for processing of personal data is the obligation arising from legal provisions (in accordance with Article 6(1)(c) of the GDPR)** **f) Providing personal data is voluntary and has been initiated by the Whistleblower.** **g) Personal data will be stored for no longer than 3 years from the completion of follow-up actions or from the date of the decision that the report is groundless.** **h) The reporting person has the right to:** **a) obtain information about the processed personal data,** **b) object to the processing of personal data (request to stop data processing),** **c) correct and update data,** **d) restrict processing,** **e) file a complaint with the President of the Office for Personal Data Protection,** **i) We do not plan to engage in profiling, nor will we transfer data to third countries.** **j) Data will not be disclosed to anyone during the execution of actions covered by the report unless required by applicable law or necessary for the proper receipt and handling of the report (e.g., hosting or IT services).**

***Appendix no. 4 to the procedure for reporting breaches of the law and taking follow-up actions in the Luma Group*.**

Internal Report Register

No.	Date of receipt of the report	Report number	Reporting person's data / anonymous	Contact address	Consent for disclosure of data yes/no	Subject of the breach of law	Person concerned	Date of receipt of the report	Date of reply	Follow-up actions	Date of case closure	Appendices to the report/notes

WHISTLEBLOWERS PROCEDURE

REPORTING OF BREACHES

KUTNO FOUNDRY
powered by Luma Automation

What is subject to report

The reportable violations include breaches of law or unlawful omissions aimed at circumventing the law concerning:

- corruption;
- public procurement;
- financial services, products and markets;
- prevention of money laundering and terrorist financing;
- product safety and compliance;
- transport safety;
- environmental protection;
- public health;
- consumer protection;
- oprotection of privacy and personal data;
- security of network and information systems;
- the financial interests of the State Treasury of the Republic of Poland, local government units, and the European Union;
- the internal market of the European Union, including public law rules on competition and state aid, as well as corporate taxation;
- breaching applicable regulations, procedures, customs, and ethical standards established by the legal entity within the Luma Group.

1 Reporting of a breach

→ **Reports are to be received by the Audit Department of Luma Services Sp. z o.o.**

Reports should be submitted to the email address **sygnalista@lumaservices.eu**. You may use the form attached to the procedure (Appendix No. 2) for this purpose.

→ **In the event that the report of a breach pertains to the Audit Department, the report should be submitted via email to the following address zarzad@lumaservices.eu.**

→ **The report should primarily include:**

- reporting date;
- reporting person's details, i.e., first name, last name, contact email address;
- indication of the work-related context;
- job position of the reporting person;
- person concerned;
- details of the individuals who committed the breach of law, i.e., first name, last name, position, and workplace;
- a description of the irregularities and the dates on which they occurred.

It is also advisable to document the report with collected evidence and a list of witnesses.

2 Follow-up actions

→ Follow-up actions will be conducted as needed by the Legal Department, Accounting Department, and Audit Department of Luma Services Sp. z o.o.

→ The reporting person will receive confirmation of the report's receipt **within 7 days of its submission.**

→ Within 3 months of the confirmation of receipt of the report, the reporting person will be provided with a feedback.

! Anonymous reports are not processed.

! Additional Remarks

→ Retaliatory measures or attempts or threats to take such actions against the whistleblower or facilitators in making the report are prohibited. These actions include, but are not limited to, intimidation, dismissal, withholding promotion or demotion, suspension, negative performance evaluations, discrimination, unfavourable changes to work location or hours, financial penalties, etc.

→ The whistleblower's personal data, which may reveal their identity, will not be disclosed to unauthorised individuals unless the whistleblower gives explicit consent or it is required by law.

→ The whistleblower is liable for false reports if they are aware that no legal breach has occurred.