Annex No. 3 to the Minutes of the Meeting of the Management Board of Talkersi.pl Sp. z o.o. based in Gdynia, dated 16 December 2025

Internal Whistleblowing Procedure Talkersi.pl Sp. z o.o. *(consolidated text)*

§ 1 Definitions

1. Legal Entity or Employer – Talkersi.pl Sp. z o.o. with its registered office in Gdynia, at ul. Łużycka 10, 81-537 Gdynia, entered into the Register of Entrepreneurs of the National Court Register maintained by the District Court Gdańsk-Północ in Gdańsk, 8th Commercial Division of the National Court Register under KRS number: 0000544763, NIP: 5862294976, REGON: 360825279, with a share capital of PLN 5,000.00.
2. Procedure – shall mean this internal whistleblowing procedure specifying the rules for reporting breaches of law and taking follow-up actions.
3. Act – shall mean the Act of 14 June 2024 on the Protection of Whistleblowers (Journal of Laws of 2024, item 928).
4. Information on a breach of law – shall mean information, including reasonable suspicion, regarding an actual or potential breach of law that has occurred or is likely to occur within the legal entity where the whistleblower participated in the recruitment process or other pre-contractual negotiations, works or worked, or within another legal entity with which the whistleblower maintains or maintained contact in a work-related context, or information concerning an attempt to conceal such a breach of law.
5. Internal report – shall mean the communication of information on breaches in accordance with this Procedure.
6. External report – shall mean the communication of information on a breach of law to the Commissioner for Human Rights (*Rzecznik Praw Obywatelskich*) or another public authority.
7. Public disclosure – shall mean making information on a breach of law available to the public.
8. Work-related context – shall mean past, present, or future activities related to the performance of work under an employment relationship or other legal relationship constituting the basis for providing work, services, or performing functions within or for a legal entity, within the framework of which information on a breach of law was obtained and there is a risk of experiencing retaliation.
9. Person concerned – shall mean a natural person, a legal person, or an organizational unit without legal personality to which the law grants legal capacity, identified in the report or public disclosure as a person who committed the breach of law or as a person associated with the person who committed the breach.
10. Follow-up action – shall mean action taken by the legal entity to assess the accuracy of the allegations contained in the report and to address the breach of

law that is the subject of the report, in particular through verification of the report and provision of feedback.

11. Feedback – shall mean information provided to the whistleblower on the follow-up action planned or taken and the grounds for such action.
12. Retaliation – shall mean any direct or indirect action or omission occurring in a work-related context, prompted by a report or public disclosure, which infringes or may infringe the rights of the whistleblower, or which causes or may cause unwarranted harm to the whistleblower, including the groundless initiation of proceedings against the whistleblower.
13. Facilitator – shall mean a natural person who assists a whistleblower in the reporting process or public disclosure in a work-related context and whose assistance should remain confidential.
14. Person connected with the whistleblower – shall mean a natural person who may experience retaliation, including a co-worker or a relative of the whistleblower within the meaning of Article 115 § 11 of the Criminal Code Act of 6 June 1997 (Journal of Laws of 2024, item 17).

§ 2 Whistleblower

1. A whistleblower is a natural person who reports or publicly discloses information on a breach of law acquired in a work-related context, including:

a) An employee,
b) A temporary agency worker,
c) A person providing work under a basis other than an employment relationship, including a civil law contract,
d) An entrepreneur,
e) A holder of a commercial power of attorney (prokurent),
f) A shareholder or partner,
g) A member of a body of a legal person or an organizational unit without legal personality,
h) A person working under the supervision and direction of a contractor, subcontractor, or supplier,
i) A trainee,
j) A volunteer,
k) An intern.

2. This Procedure also applies to a whistleblower reporting or publicly disclosing information on a breach of law acquired in a work-related context prior to the establishment of an employment relationship or other legal relationship constituting the basis for work, services, or holding a position, or after its termination.

3. A whistleblower shall qualify for protection provided under Chapter 2 of the Act from the moment of making a report (internal or external) or public disclosure, provided that they had reasonable grounds to believe that the information subject to the report or disclosure was true at the time of reporting and that it constituted information on a breach of law.

4. The protection specified in Chapter 2 of the Act applies accordingly to:

1. A facilitator,
2. A person connected with the whistleblower,
3. A legal person or other organizational unit assisting or connected with the whistleblower, in particular owned by or employing the whistleblower.

§ 3 Breaches of Law Covered by the Procedure

A breach of law is an unlawful act or omission, or an act 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. Radiation protection and nuclear safety,
9. Food and feed safety,
10. Animal health and welfare,
11. Public health,
12. Consumer protection,
13. Protection of privacy and personal data,
14. Security of network and information systems,
15. Financial interests of the State Treasury of the Republic of Poland, local government units, and the European Union,
16. Internal market of the European Union, including public competition rules, state aid rules, and corporate taxation,
17. Constitutional freedoms and human and civil rights – occurring in relations between an individual and public authorities, unrelated to the fields listed in items 1–16 above.

§ 4 Internal Reporting Team

1. The Internal Reporting Team (hereinafter: the "Team") receives internal reports and carries out follow-up actions.
2. The Team consists of:

a) Chief Operating Officer (COO) – decision-maker,

b) HR Lead – handler of internal reports in accordance with the Procedure.

3. In case of doubt or division within the Team, the Chief Operating Officer holds the casting vote.
4. Members of the Team hold written authorization issued by the Employer, the template of which constitutes Annex No. 1 to the Procedure.
5. Members of the Team are obliged to maintain confidentiality regarding all information and personal data obtained during the receipt and verification of

internal reports and follow-up activities, including after the termination of their employment or other legal relationship under which they performed work.

§ 5 Submission Methods

1. Reports of breaches may be submitted electronically to the email address: kadry@talkersi.pl, using the form set out in Annex No. 2 to the Procedure, providing a contact email address in the designated field. In the case of reports involving alleged breaches by members of the Team, the report must be submitted using the aforementioned form electronically to the email address of a member of the Employer's Management Board. The Management Board shall process the report applying this Procedure accordingly.
2. Anonymous reports will not be accepted.

§ 6 Confidentiality

The Employer prevents unauthorized persons from obtaining access to information contained in an internal report and ensures protection of the confidentiality of the identity of the whistleblower, the person concerned, and any third party mentioned in the report. Protection of confidentiality applies to information from which the identity of such persons can be directly or indirectly identified.

§ 7 Follow-up Action

1. Follow-up action, including the verification of the internal report and further communication with the whistleblower (such as requesting additional information and providing feedback), is carried out impartially by the Team.
2. The Team is obliged to:

1) Acknowledge receipt of the internal report to the whistleblower within 7 days of its receipt, unless the whistleblower has not provided a contact address,
2) Take actions to verify the report,
3) Provide feedback to the whistleblower within a timeframe not exceeding 3 months from the date of acknowledgement of receipt, or, if no acknowledgement was provided, within 3 months from the expiry of 7 days following the submission of the report, unless the whistleblower has not provided a contact address.

3. Following verification, the Team may recommend, in particular, the following remedial measures:

1) Organizational support:
    a) Amendments to existing procedures,
    b) Adjustments to the organizational structure,
    c) Reassignment within existing structures,
    d) Referral for training,
    e) Referral for mediation.
2) Other measures:
    a) Formal documented conversation,
    b) Performance improvement / corrective plan,

c) Disciplinary warning/penalty,
d) Termination of employment or other agreement with notice,
e) Summary dismissal / termination of employment or other agreement without notice.

3) Support for the whistleblower, facilitator, or connected person:
   a) Psychological support.
4) Escalation of the report:
   a) Filing a notification of suspected criminal or petty offense,
   b) Initiating other legal proceedings (e.g., filing a lawsuit).

§ 8 Register of Internal Reports

1. The Team maintains a Register of Internal Reports.
2. The Employer acts as the Data Controller for personal data contained in the register.
3. The Register of Internal Reports includes:
   1) Report reference number,
   2) Subject matter of the breach,
   3) Personal data of the whistleblower and the person concerned, necessary for identification,
   4) Contact address of the whistleblower,
   5) Date of internal report,
   6) Information on follow-up actions taken,
   7) Date of case closure.
4. Personal data and other information in the register shall be stored for a period of 3 years after the end of the calendar year in which follow-up actions were completed or after the conclusion of proceedings initiated by these actions.
5. A template of the Register of Internal Reports constitutes Annex No. 3 to the Procedure.

§ 9 Processing of Personal Data

1. The personal data of the whistleblower allowing for their identification shall not be disclosed to unauthorized persons without the explicit consent of the whistleblower.
2. The Employer is, however, obliged to disclose the whistleblower's personal data upon request of a public authority or court where such disclosure is a necessary and proportionate obligation under applicable law in connection with investigations conducted by those authorities or pre-trial or judicial proceedings. Before making such disclosure, the competent public authority or court shall notify the whistleblower, providing written or electronic explanation of the reasons for disclosure, unless such notification would jeopardize the investigation or court proceedings.
3. Upon receiving a report, the Employer shall process personal data only to the extent necessary to receive the report or carry out follow-up action. Personal data irrelevant to the handling of the report shall not be collected, and if collected

accidentally, shall be deleted immediately (within 14 days of determining its irrelevance).
4. Article 14(2)(f) of Regulation (EU) 2016/679 (GDPR) does not apply, unless the whistleblower fails to meet the legal requirements for protection or has given explicit consent to the disclosure of their identity.
5. Article 15(1)(g) of the GDPR regarding the provision of information on the source of personal data does not apply, unless the whistleblower fails to meet the legal requirements for protection or has given explicit consent to such disclosure.
6. Personal data processed in connection with receiving a report or taking follow-up action, alongside documentation, shall be stored by the Employer for 3 years after the end of the calendar year in which follow-up action was completed or proceedings concluded.
7. After the expiration of the period specified in paragraph 6, the Employer shall delete personal data and destroy documents related to the report. The Act of 14 July 1983 on National Archival Resources and Archives does not apply.
8. Paragraph 7 does not apply if documents related to the report form part of files of ongoing pre-trial, court, or administrative court proceedings.
9. The GDPR Information Clause constitutes Annex No. 4 to the Procedure.
10. The Information Clause will be sent upon reporting to the provided email address and to individuals whose data was obtained from the reporting person.

§ 10 External Reporting Information

1. Reports may also be submitted directly to the Commissioner for Human Rights (*Rzecznik Praw Obywatelskich*) or a public authority, bypassing the internal procedure, or – where appropriate – to European Union institutions, bodies, or agencies.
2. Contact details for the Commissioner for Human Rights (RPO):
    - Citizen Helpline: 800 676 676
    - Email: biurorzecznika@brpo.gov.pl
    - Address: Biuro RPO, al. Solidarności 77, 00-090 Warszawa
3. Further details regarding external reporting are specified in Chapter 4 of the Act.

§ 11 Final Provisions

1. These regulations were agreed with representatives of persons performing work for the Employer, selected in accordance with the procedure adopted by the Employer.
2. The regulations enter into force within one week from the date of announcement in the manner adopted by the Employer.
3. Every person performing work under an employment relationship or other legal relationship shall confirm via email or in writing that they have read and understood this procedure.
4. Any job applicant shall be provided with information on the internal whistleblowing procedure upon commencing recruitment or pre-contractual negotiations.

.....

[Signature on behalf of Employer]

Consulted with: .....

[Signatures of staff representatives]

Annexes

1. Template Authorization to Process Personal Data
2. Template Internal Reporting Form
3. Template Register of Internal Reports
4. GDPR Information Clause

Annex No. 1 – Authorization to Process Personal Data Template

Gdynia, date: [Date]

Talkersi.pl Sp. z o.o.

ul. Łużycka 10, 81-537 Gdynia

KRS: 0000544763 | NIP: 5862294976 | REGON: 360825279

To:

Mr./Ms. [Name]

Obligation and Authorization

I hereby inform you that in connection with your position and based on the internal whistleblowing procedure implemented within the legal entity, you are appointed as a member of the Internal Reporting Team, and I hereby instruct you to perform your duties in accordance with the said procedure.

I hereby authorize you to process personal data in accordance with the internal whistleblowing procedure.

Simultaneously, please be advised that members of the Team are required to maintain strict confidentiality regarding information and personal data obtained during the receipt, verification, and follow-up handling of internal reports, including after the termination of employment or other contractual relationship (Art. 27(2) of the Act of 14 June 2024 on the Protection of Whistleblowers).

Annex No. 2 – Internal Reporting Form Template

Internal Report
Date of report:
Full Name: Position: Department/Unit: Contact email address:
Date of occurrence of the breach: Date whistleblower became aware:
Description of the breach: *(Please describe in detail the circumstances of the breach, specifying time, location, persons involved, potential witnesses, how knowledge was acquired, and all relevant details)*
Indication of specific legal provisions breached:
List of witnesses (including contact details):
List of relevant documents (please attach or indicate who holds them):
Whistleblower's Statement I hereby declare that: 1. I have read and understood the Internal Whistleblowing Procedure. 2. I have reasonable grounds to believe that the information reported is true and constitutes a breach of law. 3. I am acting in good faith and not for personal gain.

Annex No. 3 – Register of Internal Reports Template

Internal Report Register

no.	Subject of the breach	Whistleblower's personal details	Whistleblower's contact details	Personal data of the person concerned	Date of internal report	Information on follow-up actions taken

Annex No. 4 – GDPR Information Clause

1. The controller of your personal data is **Talkersi.pl Sp. z o.o.** with its registered office in Gdynia, at ul. Łużycka 10, 81-537 Gdynia, entered into the Register of Entrepreneurs of the National Court Register maintained by the District Court Gdańsk – Północ in Gdańsk, 8th Commercial Division of the National Court Register under KRS number: 0000544763, NIP: 5862294976, REGON: 360825279, with a share capital of PLN 5,000.00.
2. **Controller contact details:** kadry@talkersi.pl.
3. Your personal data will be processed for the purpose of receiving the report and conducting explanatory proceedings based on a legal obligation to which the controller is subject under the Act of 14 June 2024 on the Protection of Whistleblowers.
4. **Protection of the whistleblower's identity:** Your personal data shall not be disclosed to unauthorized persons, unless with your explicit consent. In connection with explanatory proceedings conducted by public authorities or preparatory/court proceedings conducted by courts, including for the purpose of guaranteeing your right of defense, your data may be disclosed when such action constitutes a necessary and proportionate obligation resulting from the provisions of law. Prior to such disclosure, the competent public authority or competent court shall notify you, sending in paper or electronic form an explanation of the reasons for the disclosure of personal data. The notification shall not be sent if it may jeopardize the explanatory, preparatory, or court proceedings.
5. The Controller ensures the confidentiality of your data in connection with the received report.

6. Personal data processed in connection with receiving a report or taking follow-up actions, as well as documents related to this report, shall be stored for a period of 3 years after the end of the calendar year in which the report was submitted or follow-up actions were completed, or after the completion of proceedings initiated by these actions. Personal data that is not relevant to the handling of the report shall not be collected, and if collected accidentally, shall be deleted without delay. Deletion of such personal data shall take place within 14 days from the moment of determining that it is irrelevant to the case.
7. You have the right to request access to your personal data, as well as its rectification (correction). You also have the right to request the erasure or restriction of processing, as well as the right to object to processing; however, these rights apply only if further processing is not necessary for the Controller to comply with a legal obligation and there are no other overriding legal grounds for processing.
8. You have the right to lodge a complaint regarding the processing carried out by the Controller with the President of the Personal Data Protection Office (uodo.gov.pl).