

---

# **Common Procedure for Reporting Breaches and Whistleblower Protection**

---

Warsaw, February 2025

## I. General provisions

- 1.1. This Procedure has been adopted based on the provisions of the Act of 14 June 2024 on the protection of whistleblowers and applies to the entities listed in Annex No. 1. The procedure is a common internal reporting procedure under Article 28 sec. 8 of the Act of 14 June 2024 on the protection of whistleblowers.
- 1.2. The purpose of the Procedure for Reporting Breaches and Whistleblower Protection is to enable persons identified in the Procedure to report breaches of the law in a work-related context and to provide appropriate and effective protection against retaliatory actions against whistleblowers.
- 1.3. The Procedure specifies, among other things, the rules for internal reporting understood as providing information about a law breach, managing such reports and taking follow-up actions in accordance with the Act of 14 June 2024 on the protection of whistleblowers.

## II. Definitions

- 2.1. The terms used in the Procedure mean:
  - (i) **Contact address** – an e-mail address provided for by the Whistleblower;
  - (ii) **Follow-up actions** – actions taken to assess the accuracy of the allegations in the Report and to address the Breach that is the subject of the Report, in particular by conducting an internal enquiry;
  - (iii) **Retaliation** – a direct or indirect act or omission in a work-related context that is prompted by an internal report, external report or public disclosure and that violates or may violate the rights of the Whistleblower or causes or may cause unjustified detriment to the Whistleblower, including unfounded initiation of proceedings against the Whistleblower;
  - (iv) **Information on a Breach** – an information, including a reasonable suspicion about actual or potential Breaches that occurred or are likely to occur in the Company;
  - (v) **Feedback** – an information provided to the Whistleblower on envisaged or taken as Follow-up actions and the grounds for such actions;
  - (vi) **Other illegal activities** – any other breaches of law occurring within the Company in the Work-related context, not covered by the catalogue defined under the definition of the Breach in the Procedure and violations of internal regulations and ethical standards applicable in Medicover at the local or international level;
  - (vii) **Coordinator** – a person or persons authorised by the Company to receive Reports, to take Follow-up actions, to maintain the Register of Reports, and to ensure compliance with legal provisions of the processes and tasks from the Procedure;
  - (viii) **Work-related context** – past, current or future activities related to the performance of work under an employment or any other relationship constituting the basis for the provision of work, services or functions in the Company or for the Company, through which information about a Breach was acquired and there is a possibility of experiencing Retaliation;
  - (ix) **Breach** – an action or omission that is contrary to law or is intended to circumvent the law, relating exclusively to:
    - corruption;
    - public procurement;
    - financial services, products, and markets;

- prevention of money laundering and terrorist financing;
  - product safety and compliance;
  - transport safety;
  - protection of the environment;
  - radiological protection and nuclear safety;
  - food and feed safety;
  - animal health and welfare;
  - public health;
  - consumer protection;
  - protection of privacy and personal data;
  - security of networks and tele information systems;
  - financial interests of the State Treasury of the Republic of Poland, local self-government, and the European Union;
  - the European Union internal market, including public law rules on competition, state aid and corporate taxation;
  - constitutional freedoms and rights– occurring in relations between an individual and public authorities and not related to the areas indicated in the points above;
- (x) **Person concerned**– a natural or legal person, or an entity , who is referred to in the Report or public disclosure as a person to whom the Breach is attributed or with whom that person is associated;
- (xi) **Facilitator** – a natural person who assists a Whistleblower in making a Report and whose assistance should be confidential;
- (xii) **WhistleB Platform** – a dedicated tool enabling the receipt of Reports via a form, ensuring anonymity and confidentiality, available at the address available at Our Medicover (link) as well as on the respective publicly accessible websites of the Companies under ‘Whistleblower Protection’ ;
- (xiii) **Procedure** – Common Procedure for Reporting Breaches and Protecting Whistleblowers applicable to entities listed in Annex No. 1;
- (xiv) **Register of Reports** –a register of Reports kept in electronic or paper form;
- (xv) **Company** – an entity indicated in Annex No. 1;
- (xvi) **Whistleblower** – a natural person who reports or publicly discloses Information on a Breach acquired in a Work-related context, including:
- an employee;
  - a temporary worker;
  - a person performing work on a basis other than an employment relationship, including a civil law contract;
  - an entrepreneur;
  - a person who is a member of statutory bodies and a proxy of a Company;
  - a partner of a Company;
  - a person performing work under the supervision and direction of a contractor, subcontractor or supplier;
  - a trainee;
  - a volunteer;
  - an apprentice;

- natural persons referred to above, who make a Report on information about a Breach acquired 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 performing a function in or on behalf of the Company;
- (xvii) **Whistleblower Protection Act** - Act of 14 June 2024 on the protection of whistleblowers;
- (xviii) **Report** – an internal report made by a Whistleblower in the manner and under the principles specified in the Procedure in Chapter III, of information on a Breach.

### III. Means of Submitting Reports

- 3.1.** In the event of a justified suspicion of a Breach, a Whistleblower is entitled to make a Report. A Report may be submitted via a secure form on the WhistleB Platform at the address available at Our Medicovert (link) as well as on the respective publicly accessible websites of the Companies under ‘Whistleblower Protection’.
- 3.2.** Each Report is subject to registration in the Register of Reports, regardless of who made it and whom and what a Report concerns. Incomplete Reports are also subject to registration to the extent that the information provided enables the consideration of a Report and its verification in order to determine whether a Breach occurred and to take Follow-up actions.
- 3.3.** In order to ensure a fair, objective and swift consideration of a Report, a Report shall include:
- (i) an indication of a department, team or organizational unit, in which a Breach occurred;
  - (ii) an indication of an entity, which a Report concerns and, if applicable, a person or persons associated with the matter;
  - (iii) a date or an approximate period of occurrence or discovery of the Breach;
  - (iv) a description of the irregularity (i.e. a concise description of the matter, indicating relevant facts; what the irregularity concerns, when and where it took place or may take place);
  - (v) any evidence (in any format) that may constitute evidence of an Breach;
  - (vi) any other additional information related to a Report, including in particular information on any witnesses to a Breach;
  - (vii) contact details for providing Feedback – an e-mail address;
  - (viii) a name, surname and position of a Whistleblower (unless a Report is anonymous);
  - (ix) an information whether a Whistleblower consents to the disclosure of his or her identity.
- 3.4.** A Whistleblower has the right to submit the Report anonymously.
- 3.5.** A Report may be of the following nature:
- (i) **public** – the identity of a Whistleblower may be disclosed only on the basis of an unambiguous consent expressed in a Report by the Whistleblower;
  - (ii) **confidential** – in the case of a confidential report, the confidentiality of the Whistleblower’s data is ensured, which means that no information is disclosed to unauthorised persons that could directly or indirectly identify a Whistleblower.
- 3.6.** The Report may be of the following nature:

- (i) **personal** – in situations when a Whistleblower provides his/her personal data or the Whistleblower's personal data may be determined based on the content of a Report;
  - (ii) **anonymous** – in situations when a Whistleblower does not provide his/her personal data and at the same time it is not possible to determine the Whistleblower's personal data based on the content of a Report.
- 3.7.** A Report on Other illegal activities witnessed by a Whistleblower and not covered by the Procedure is possible on the basis of separate internal regulations in force in Medcover at the local or international level. The provisions of the Whistleblower Protection Act do not apply to Reports concerning Other illegal activities.
- 3.8.** The Procedure may not be used to provide false information or to report matters relating to the private lives of employees or conflicts between employees, unless such conflicts are closely related to the Company's activities and have led to a Breach. The Procedure and the Whistleblower Protection Act do not apply to information covered by the physician-patient or attorney-client privilege.

#### **IV. Receiving of Reports**

- 4.1.** Within 7 days of receiving a Report, the Coordinator:
- (i) registers the Report in the Register of Reports;
  - (ii) performs an initial analysis of a Report; the purpose of the initial analysis is to ensure that a Report contains all the information necessary for its consideration and to determine whether the matter covered by a Report may constitute a Breach; if any deficiencies are noticed, the Coordinator contacts a Whistleblower;
  - (iii) confirms the receipt of a Report for further consideration within an internal enquiry and provides the a Whistleblower with information on the rights and obligations and on further stages of the proceedings concerning a Report, or refuses to accept a Report for further consideration and provides a Whistleblower with appropriate information.
- 4.2.** The Coordinator may refuse to accept a Report for further consideration, in particular if a Report:
- (i) violates the provisions of the Procedure; or
  - (ii) is clearly unfounded or unreliable; or
  - (iii) due to its content, it prevents the initiation of internal enquiry, and obtaining the necessary missing information is impossible.
- 4.3.** At the moment of providing information about the refusal to accept a Report, a Report is closed and the date of completion of consideration of a Report is recorded in the Register of Reports.

#### **V. Internal enquiry**

- 5.1.** The internal enquiry may be conducted by the Coordinator or, if the nature of a Report so requires, by a Committee, which work is coordinated and supervised by the Coordinator.
- 5.2.** The Commission consists of persons selected by the Coordinator. The composition of the Committee should be appropriate to the consideration of a Report and ensure objectivity and professionalism in considering a Report.

- 5.3.** If a Report concerns the Coordinator, the Coordinator shall not conduct internal enquiry or select members of the Committee. In such a situation, the composition of the Committee is each time appointed by the Management Board of Medicover Sp. z o. o.
- 5.4.** A Person concerned, a person who is a direct supervisor of a Whistleblower, not a person directly subordinate to a Whistleblower, as well as any person who may not be impartial during the internal enquiry, shall not be appointed to the Committee.
- 5.5.** The Coordinator may appoint independent consultants as members of the Committee or engage them in any other capacity, if their experience and knowledge may be helpful during the internal enquiry.
- 5.6.** The internal enquiry conducted by the Coordinator or by the Committee under the supervision of the Coordinator are conducted in accordance with the following principles: confidentiality, impartiality, due diligence and the pursuit of comprehensive and fair consideration of the collected evidence in order to clarify the circumstances indicated in the Report.
- 5.7.** During the internal enquiry, the Commission takes appropriate actions, adequate to the content of a Report, including: deposing a Whistleblower and a Person concerned; collecting witness statements; collecting documents and information.
- 5.8.** Due to the confidentiality of the internal enquiry, all members of the Committee are obliged to keep confidential the information obtained during or in connection with the consideration of a Report.
- 5.9.** All decisions of the Commission are taken by a simple majority vote. In the event of an equal number of votes, a vote of a person designated as chairman of the Commission shall be decisive.
- 5.10.** The internal enquiry should be completed within 45 days from the date of confirmation of receipt of a Report. In particularly justified situations, the internal enquiry may be extended, up to maximum of 60 days.
- 5.11.** Within 14 days of the completion of the internal enquiry, the Coordinator or the Committee under the supervision of the Coordinator shall prepare a report, which shall be signed by all members of the Committee. The purpose of the report is to summarize the internal enquiry and present conclusions and recommendations.
- 5.12.** The Coordinator submits the conclusions of the internal enquiry along with recommendations to the Management Board of a Company, which a Report concerns.
- 5.13.** Based on the information provided, the Management Board of a Company, which a Report concerns, decides on implementing actions aimed at eliminating the effects of the identified Breach, which was the subject of a Report, and on prevention of similar breaches in the future. Activities may include in particular:
  - (i) taking appropriate legal actions against persons responsible for the Breach (e.g. termination of an employment contract, notification of law enforcement authorities of a suspected crime);
  - (ii) undertaking training and educational activities;
  - (iii) modification of existing internal procedures in order to increase the effectiveness of preventive and control mechanisms.
- 5.14.** The Management Board of a Company, which a Report concerns, shall immediately provide the Coordinator with information on the actions that have been implemented in a Company in order to eliminate the effects of the identified Breach or to prevent similar breaches in the future.

- 5.15.** Feedback to a Whistleblower shall be provided by the Coordinator no later than within 3 months from the date of confirmation of receipt of a Report, provided that a Whistleblower has provided a contact address, and in the event of the lack of confirmation within 3 months from the expiry of 7 days from the date of making a Report.

## **VI. Register of Reports**

- 6.1.** The Register of Reports is kept by the Coordinator separately for each Company.
- 6.2.** The Register of Reports records all cases of Reports submitted in accordance with the principles specified in the Procedure in Chapter III. The Register of Reports is maintained in a reliable manner and reflects the actual course of actions.
- 6.3.** The Register of Reports contains:
- (i) a Report's number;
  - (ii) subject of a Breach;
  - (iii) personal data of a Whistleblower (unless a Report is anonymous) and a Person concerned;
  - (iv) a Contact address of a Whistleblower;
  - (v) a date of submission of a Report;
  - (vi) an information about Follow-up actions;
  - (vii) a date of completion of the proceedings concerning a Report.
- 6.4.** The Coordinator, separately for each Company, keeps documentation regarding a Report and Follow-up Actions.
- 6.5.** Personal data, other information in the Register of Reports and documentation are retained 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 proceedings initiated by Follow-up actions.

## **VII. Whistleblower Protection**

- 7.1.** The Whistleblower's personal data allowing for his/her identification shall not be disclosed, unless a Whistleblower consents to the disclosure of his/her identity. The above principle does not apply when a disclosure is a necessary and proportionate obligation under the law in connection with investigations conducted by public authorities or judicial proceedings conducted by courts, including in order to safeguard the right of defence of a Person concerned. Before making the disclosure, a competent public authority or court shall notify a Whistleblower by sending a statement of reasons for disclosing his or her personal data in paper or electronic form, unless such notification would jeopardise the investigation, or court proceedings.
- 7.2.** No Retaliation may be taken against a Whistleblower (whose work was, is or is to be performed under an employment contract), including threats of Retaliation or attempts of Retaliation. It is prohibited to make Retaliation, in particular involving:
- (i) a refusal to enter into an employment relationship;
  - (ii) a notice of termination or termination without notice of the employment relationship;
  - (iii) a failure to conclude a fixed-term employment contract or an employment contract for an indefinite period after 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 after the termination of a fixed-

term employment contract – in a situation when a Whistleblower had a justified expectation that such a contract will be concluded with him/her;

- (iv) a reduction of the remuneration for work;
- (v) a withholding of promotion or omission for promotion;
- (vi) an omission when granting work-related benefits other than remuneration or reducing the amount of such benefits;
- (vii) a transfer to a lower job position;
- (viii) a transfer of current duties of a Whistleblower to another employee;
- (ix) a suspension from the performance of employment or service duties;
- (x) an unfavourable change in the place of work or working time schedule;
- (xi) a negative evaluation of work results or negative opinion about work;
- (xii) an imposition of a disciplinary measure, including a financial penalty, or a measure of a similar nature;
- (xiii) a coercion, intimidation or exclusion;
- (xiv) mobbing;
- (xv) a discrimination;
- (xvi) an unfavourable or unfair treatment;
- (xvii) a suspension of participation or omission when selecting for participation in training to improve professional qualifications;
- (xviii) an unjustified referral for a medical examination, including psychiatric examination, unless separate provisions provide for the possibility of referring an employee to such an examination;
- (xix) any action aimed at making it more difficult to find future employment in a given sector or industry on the basis of an informal or formal sectoral or industry agreement;
- (xx) causing financial loss, including economic loss or loss of income;
- (xxi) causing other non-material damage, including infringement of personal rights, in particular the good name of a Whistleblower.

**7.3.** The prohibition of making Retaliation specified in sec. 7.2 above shall apply accordingly if the work, provision of services or performance of a function was, is or is to be performed on the basis of a legal relationship other than an employment relationship, unless the nature of the work, service or function does not exclude the application of such action towards a Whistleblower.

**7.4.** A Whistleblower is protected from the moment of making an internal Report, an external report or public disclosure, provided that a Whistleblower had reasonable grounds to believe that the information that was the subject of the internal Report, external report or public disclosure was or public disclosure is true at the time of internal reporting, external reporting or public disclosure and that it constitutes information about a Breach.

**7.5.** The whistleblower protection provided for in the Procedure does not apply in the event of reporting Other illegal activities or making an internal report, an external report or public disclosure in bad faith, in particular falsely or untruly.

## **VIII. External Reports**

**8.1.** The WhistleB Platform, used for a secure and confidential receipt of Reports, has been made available to quickly and effectively respond to Breaches and to prevent their

occurrence in the future, ensuring the protection of a Whistleblower. If you are aware of any Breaches, we encourage you to submit such information via the WhistleB Platform .

- 8.2.** Regardless of the provisions of this Procedure, a Whistleblower is entitled to make external reports. An external report may be made either after a Whistleblower has made an internal Report of a Breach in a Company in the manner and under the principles specified in the Procedure, or without such a report.
- 8.3.** External reports should be addressed to the Ombudsman or to public authorities and, when appropriate, to institutions, bodies, offices or agencies of the European Union.
- 8.4.** Up-to-date information on external reporting procedures and contact details for making external report are available on the websites of the relevant authorities, institutions, offices or agencies.

## **IX. Personal data**

- 9.1.** Personal data obtained to the extent necessary to receive a Report or take any Follow-up actions will be processed by the Administrator (i.e. a Company, which a Report concerns) and authorized persons.
- 9.2.** Personal data that is not relevant to the processing of Reports is not collected, and in the event of accidental collection, it is immediately deleted. These personal data are deleted within 14 days from the moment it is determined that they are irrelevant to the case.
- 9.3.** All personal data processed as a result of receiving a Report, including in particular the personal data of a Whistleblower, a Person concerned, witnesses and experts, are subject to legal protection in accordance with the relevant legal provisions.

## **X. Final provisions**

- 10.1.** A person applying for employment under an employment relationship or another legal relationship constituting the basis for the provision of work or services or performing a function in the Company is provided with information on the Procedure at the beginning of recruitment or negotiations preceding the conclusion of a contract.
- 10.2.** The content of the Procedure was adopted after consultations within a Company.
- 10.3.** The Procedure comes into force after 7 days from the date of its announcement to persons performing work in the manner accepted in a Company.
- 10.4.** Annex No. 1 containing the list of Companies covered by the Common Procedure for Reporting Breaches and Whistleblower Protection will be subject to periodic updates in the event of the adoption of the Procedure by another entity. Amending content of Annex No. 1 does not constitute a change to the content of the Procedure and does not require re-adoption by the Companies.

Annex No. 1: List of Companies Covered by the Common Procedure for Reporting Breaches and Whistleblower Protection:

1. Centrum Medyczne Damiana Holding sp. z o.o.;
2. Centrum Medyczne MML sp. z o.o.;
3. Medicover sp. z o.o.;
4. Medicover Benefits sp. z o.o. ;
5. Medicover Sport sp. z o.o.;
6. Medicover Forsakrings AB (PUBL)Spółka Akcyjna - Oddział w Polsce;
7. Invimed - T sp. z o.o. ;

8. Care Experts sp. z o.o.;
9. Medi Partner sp. z o.o.;
10. Elford sp. z o.o.;
11. Well Fitness sp. z o.o.;
12. Just Gym sp. z o.o.;
13. McFit Polska sp. z o.o.;
14. Smart Platinum sp. z o.o.;
15. Medicus Uroda sp. z o.o.;
16. Centrum Diagnostyczno -Terapeutyczne „Medicus” sp. z o.o.;

.