Version Number: 1.0
Parent document: **N/A**
Title: Instruction for Internal Reporting of Breaches

Introduction

This document **(the "Manual")** describes the rules for reporting **Breaches** at Takeda SCE sp. z o.o. ("**Takeda**"), pursuant to the Whistleblower Protection Act from June 14th, 2024 (the "**Act**"). It contains information:

- What is **a Breach**, and therefore what can be reported;
- how to report **the Breach**;
- how Takeda protects **Whistleblowers,** and
- how applications are processed.

Takeda created this **Manual** because we are committed to doing business in accordance with the law and creating an ethical workplace. The principles described here are intended to detect **Breaches** and effectively counteract their effects. **Takeda** opposes all forms of retaliation against **Whistleblowers** and protects the confidentiality of their identities and reports.

How to understand the terms in this Manual?

- **Whistleblower** – a person who reports **Breaches** and meets the conditions set out in Article 4 **of the Act**
- **Whistleblowing Officer** or **WO** – the person(s) who have been designated and authorized in writing by **Takeda** to receive and investigate reports. Information on who is the **Whistleblowing Officer can** be found here: https://assets-dam.takeda.com/image/upload/v1726856997/LOC/pl-pl/CSR/Whistleblowing_Officers_Takeda_SCE.pdf

The rest of the terms that have been defined and written in capital letter and **bold** are explained in this **Instruction**.

What can be reported?

1. **A Breach** is any event that is illegal or intended to circumvent the law. **Breaches** that may be reported in accordance with **the Act** are **Breaches** occurring in the following areas:

corruption,	procurement,	services, products, and financial markets,	counteracting money laundering and terrorist financing ("**AML**"),
product safety and compliance,	transport safety,	environmental,	radiation protection and nuclear safety,
food and fodder safety,	animal health and welfare,	public health,	consumer protection,
protection of privacy and personal data,	security of networks and information and communication technology (ICT) systems,	internal market of the European Union,	public competition rules,
the financial interests of the State Treasury of the Republic of Poland, local government units and the European Union,	public aid rules,	corporate taxation,	constitutional freedoms and rights of man and citizen – occurring in the relations of an individual with public authorities.

2. **The Breach**, under **the Act,** must be related to the performance of work, the provision of services, the supply of goods to **Takeda,** or the performance of a function within **a Takeda** body.
3. **Any other event that is inconsistent with Takeda's Code of Ethics** or other policies, procedures, and instructions adopted by **Takeda is** also **a Breach.**

4. The above **Breaches** or other incidents that constitute a violation of the law, procedures or ethical standards may be reported as described in the **Global Policy on Raising & Handling Concerns**.
5. These reports will be considered in accordance with the rules described in the above-mentioned policy, therefore the provisions of this **Manual** and the requirements **of the Act** will not apply to them.
6. Therefore, you can report any **Breach** for which there is a reasonable suspicion that:
   a. happened in the past,
   b. currently or
   c. may become a reality in the future.
7. **It is important to choose the right reporting channel, which determines the manner of their consideration and the appropriate rules for the protection of the Reporter**.

How can you become a Whistleblower?

8. **A Breach** may be reported by any person who is: an employee, temporary worker, intern, apprentice, volunteer, provides services or goods to **Takeda** as an entrepreneur, performs work under the supervision and direction of a contractor, subcontractor or supplier of **Takeda**, or is a member of **Takeda's** body or its proxy.
9. You can also report **a Breach**, which occured:
   a. prior to entering into an employment relationship or other legal relationship on which the performance of work, services, goods, or functions at **Takeda** is based; or
   b. after the termination of such intercourse.

10. You can report **a Breach**:

Online	**Phone**	**At the meeting**
by submitting a report via the dedicated Ethics Line Platform (**the** "**Platform**"), available at: https://secure.ethicspoint.com/domain/media/en/gui/28267/report.html by selecting the option to file locally with the appropriate **Takeda company**.	By calling the number provided on **the Platform** and informing the person receiving the report that you want to file a local report with the relevant **Takeda company**.	By requesting a face-to-face meeting ("**Meeting**"), addressing the **Whistleblowing Officer** directly. The **WO** shall organize such a **Meeting** (in person or online) within 14 days of receipt of such a request.

11. **The platform** is available 24/7 and ensures complete data confidentiality. Unauthorised persons cannot access the information covered by the report.
12. Please note that **the Platform** is used to report all **Breaches**, it is necessary to select the local reporting option as described below. Subject to paragraphs 4 and 5, the provisions of this **Manual** and the requirements **of the Act** will not apply to reports submitted globally.
13. When reporting an online **Breach** through **the Platform**, you should:
    a. Select the "ONLINE" option, the country "POLAND", specify whether the event took place in the country where you are located and indicate the relevant Business Unit or Business Function to which **the Breach** relates.
    b. Indicate that **the Breach** relates to: "Takeda SCE (Łódź) local notification".
    c. Review your local privacy policy. Finally, select the "Continue" option.
    d. Specify the macro-category of the application.
    e. Fill in the form carefully. After filling it in, you will receive a PIN and set a password that will be used each time to log in to the application again, eventually change what has already been reported and receive feedback.
    f. **The platform** automatically sends you a notification when your request has been submitted correctly.
14. When reporting **a Breach** by phone, you should:
    a. Go to **the Platform** and select the "PHONE" option, country "POLAND".

b. Review your local privacy policy. Then you will see the phone number to call. Information on the processing of personal data and how to manage this request will be provided again.

c. Inform the operator about **the Breach**. The operation will fill in the form on **the Platform**. Specify that you want to make a local application to "Takeda SCE (Łódź)". After reporting, you must confirm the correctness of the information provided. Once the correctness is confirmed, you will be provided with a PIN and you will need to set a password that will be used each time to log in to the report again, eventually change what has already been reported and receive feedback.

d. **The platform** will automatically send you a notification that your request has been successfully submitted.

15. When reporting **a Breach** in **a Meeting:**

a. You must contact **the Whistleblowing Officer** who will arrange such **a Meeting** (in person or online) within 14 days of receipt of your request.

b. At the **Meeting**, after presenting the privacy policy, **WO** will accept the application. **The Meeting** will be documented by a recording or minutes only after the consent of the **Whistleblower**. Before signing the protocol, it should be checked and corrected (if required).

c. When **the WO** enters a report on **the Platform, the Whistleblower** will receive a PIN and set a password that will be used each time to log in to the report again, eventually change what has already been reported, and receive feedback.

d. **The platform** will automatically send you a notification that your request has been successfully submitted.

16. Reporting via **the Platform** can be made both with your personal data and anonymously. Anonymous reports are processed in the same way as reports submitted with your personal data.

SUMMARY:

A Whistleblower is only a person who meets all of the above conditions, i.e.:

- reports **a Breach**,
- does so by sending a request via **the Platform**, by phone or at **the Meeting**,
- is one of the persons listed in point 8.

Persons who are not Whistleblowers **will not be subject to** the principles described in this **Instruction.**

What are the rights of a Whistleblower?

17. Once you have submitted your application**, Takeda** ensures:
    a. conducting a thorough investigation,
    b. protection of identity and confidentiality of the fact of making a report,
    c. protection against retaliation,
    d. the right to receive feedback.
18. **The Whistleblower** also has the right to make an external report.

Fair investigation

19. Takeda guarantees that:
    a. will thoroughly explain the circumstances of the case. An impartial Inquiry Committee (**the** "**Committee**") will be set up to carefully analyse the information gathered to understand exactly what happened and what the consequences are. Members of **the Committee** may include relevant employees of **Takeda** (e.g. Chief Human Resources Officer, Finance Risk and Controls), **Takeda Group** employees (e.g. authorized persons from the Group's PAG or E&C departments) or external advisors (e.g. an external lawyer or psychologist). **The Committee** will collect evidence, review the available documents, and, if necessary, conduct interviews with persons who have knowledge of **the Infringement**, including **the Whistleblower**;
    b. reports will be investigated by impartial persons who are independent of the persons involved in the reported **Breach.** Only **persons who are not related to the case will be appointed to the Commission and this will not give rise to a conflict of interest;**
    c. after clarifying the report, appropriate follow-up actions will be taken with due diligence, such as: repairing the damage caused, changing the organizational structure or competences, or imposing penalties on persons involved in **the Breach.** If necessary, procedures and methods of operation will be changed or training will be organized to avoid similar **Breaches** in the future.

Identity protection and confidentiality of the fact of making a report

20. **Takeda** is committed to protecting the identity **of the Whistleblower**, the person to whom the report relates, and the third party named in the report. All persons who explain the report should keep confidential:
    a. the fact of their involvement in this process,
    b. any information obtained in connection with the report – this applies in particular to the personal data of the person to whom the report relates and the person who is accused of committing **the Breach** or another person indicated in the report,
    c. any action taken to clarify the report.
21. Any data that may allow the identification of **the Whistleblower** (even indirectly) may be disclosed to other persons only on the basis of **the Whistleblower's** prior, expressed consent. The exception is the disclosure of data to:
    a. competent authorities when such an obligation arises from the law (e.g. for the purposes of investigations conducted by public authorities or court proceedings – in particular to ensure the rights of defence of the person to whom the report relates);
    b. members of **the Commission** after ascertaining their impartiality and prior written authorization and confidentiality obligation – if it is necessary to clarify the matter and eliminate **the Breach**.

Remark! In the case of reports that concern the individual interests of the **Whistleblower** (e.g. he/she is a direct victim of the reported incident), it may not be possible to clarify the case without disclosing his or her identity. Such a case may require conversations with people who can guess who **the Whistleblower is** or disclosure of this information to them. In such cases, **Takeda** encourages you to consent to the disclosure of your identity in advance. **Takeda** ensures that those interviewed will be bound by confidentiality obligations and **the Whistleblower** will be protected from any form of retaliation. Otherwise, it may not be possible to explain the matter in a reliable way.

Protection against retaliation

22. Any form of retaliation is prohibited. **Takeda** will counteract any retaliation against:
    a. **Whistleblower**,

b. the person assisting **the Whistleblower** in making a report (a witness **to the Breach** who provided information about it);

c. persons related to **the Whistleblower** (family, friends and other people who are in close relations with the Whistleblower);

d. a legal entity that is owned, worked for or otherwise associated with **the Whistleblower.**

23. Retaliation should be understood as any direct or indirect act or omission that is taken against the persons indicated in the point above in connection with the report made, which does not occur for objective and duly justified reasons. Retaliation is aimed at worsening the legal or factual situation of these people and punishing them for reporting. Retaliation is also a threat or attempt to do so.

24. Anyone who experiences or knows of any retaliation should immediately report it under the same conditions as reporting **Breaches**.

Right to receive feedback

25. During the course of the proceedings, **Takeda** will keep **the Whistleblower** informed of the progress of the case:

a. receipt of the application will be confirmed – within a maximum of 7 days from its receipt;

b. **the Whistleblower** will be informed of the planned or taken follow-up and the reasons for such action – within a reasonable period of time, which will not exceed 3 months from the confirmation of receipt of the report.

26. The feedback will be posted on the **Platform**. Therefore, it is necessary to keep the PIN and password for the submitted application. You can always ask **the Whistleblowing Officer** directly for additional information about the status of your case.

Right to make an external notification

27. You can always report **a Breach** to the Ombudsman and the relevant public authorities of the Polish or European Union, bypassing the path described in this **Instruction**, in accordance with the **Act**.
28. However, **Takeda** encourages you to report **Breaches** internally first because:
    a. this Instruction has been established and a secure reporting channel is in place to effectively respond to **Breaches** and prevent them from occurring in the future;
    b. a number of rights are provided, e.g. protection against retaliation, confidentiality of reporting and identity protection, and the right to feedback;
    c. **Takeda** is closer to the people and the case to which the report relates, so it will conduct the investigation faster and more efficiently.

What are the duties of a Whistleblower?

29. After submitting your application:
    a. the proper course of the application procedure should not be disturbed,
    b. it is necessary to keep the fact of making the report confidential and all communication and information obtained related to the report,
    c. at the request of **the WO** or **the Commission** – to the extent necessary – assist in clarifying the notification.

Remark! Maintaining the confidentiality of the fact of making a report is particularly important from the perspective of the possibility of conducting an effective explanatory procedure. Disclosure of the fact of making a report will make it much more difficult to protect **the Whistleblower** from retaliation and will disrupt the work of **the WO**/ **Commission**, which should protect their identity. Such disclosure may also deprive **the Whistleblower** of the protection guaranteed by **the Act**. If **the Whistleblower** feels that the report is not being properly investigated, he/she should contact **the WO** again directly or via **the Platform**.

What is the responsibility for violating the Instructions?

30. A breach of **the Instruction** may be the basis for legal and disciplinary liability of the person who committed such a breach.
31. Criminal liability under **the Act** or disciplinary liability is subject in particular to persons who:
    d. prevent or hinder the submission of a report,
    e. take retaliatory action,
    f. breach the duty of confidentiality,
    g. knowingly report false information or assist in such reporting,
    h. make reports in bad faith, e.g. by using the reporting system for personal gain or to obtain undue protection from **Whistleblowers**.

Final provisions

32. In accordance with **the Law, Takeda** maintains a register of local internal report of breaches and is the controller of the data collected therein.
33. The following persons shall be informed of the provisions of **the Instruction**:
    a. persons applying to perform work on the basis of an employment relationship or other legal relationship constituting the basis for the provision of work or services or the delivery of goods or functions at **Takeda** along with the commencement of recruitment or negotiations prior to the conclusion of a contract,
    b. employees before they are allowed to work.
34. **The Instruction** is consulted with representatives of persons performing work. Such consultations last from 5 to 10 days from the presentation of the content of **the Instruction** to the representatives.
35. **The instruction** comes into force 7 days after it is communicated to the persons performing the work.

Version Number: 1.0
Parent document: **N/A**
Title: Instruction for Internal Reporting of Breaches

Attachments

Appendix 1: Information clause – personal data

Annex 2: General authorization

Appendix 3: Authorization for a specific case

Approval

Approver	Date	Signature
TBS Risk Lead – **Anna Stępnicka**	04-Mar-2025 | 14:45 CET	DocuSigned by: Anna Stępnicka 78542A49C4FB439...
Privacy Officer – **Cecylia Szemik**	05-mar-2025 | 11:48 CET	DocuSigned by: Cecylia Szemik 5D6CB6075549413...
Head of HR – **Jarosław Fotyga**	14-Mar-2025 | 14:56 CET	DocuSigned by: 5118367B7CE5462...
TBS Global Hub Lead in Lodz and Accounting Lead US & EUCAN - **Dariusz Adamus**	14-mar-2025 | 16:44 CET	DocuSigned by: Dariusz Adamus 7F24ED25257B4A1...

Appendix 1: Privacy Notice – personal data

Privacy Notice

1. Depending on the type of reported breaches, the Controller of the personal data provided as part of the reports is **Takeda SCE sp. z o.o**. with its registered office in Łódź, Sterlinga 8a, 91-425 Łódź (**the** "**Company**").
2. **The Company** processes personal data contained in reports in accordance with the provisions on the protection of personal data, in particular *the EU Regulation 2016/679* ("**GDPR")** and the regulations on the protection of persons reporting breaches of the law – including *the Act of 14 June 2024 on the protection of whistleblowers*.
3. Contact with **the Company** is possible at the address of the registered office indicated in point 1 above.
4. In matters related to the processing of personal data and the exercise of rights under the **GDPR,** the Whistleblower may contact the following address: privacyoffice@takeda.com.
5. **The Company** processes the personal data contained in the report: of the Whistleblower, persons to whom the report relates and other persons for purposes related to the reported cases of breaches of law, on the basis of: a legal obligation resulting from the provisions on the protection of whistleblowers (in accordance with Article 6(c) of the GDPR or if the report contains special categories of data – in accordance with Article 9(2)(g)) or the legitimate interest of the Controller, which is receiving, verifying and clarifying reports of breaches of law (in accordance with Article 6(1)(f) of the GDPR).
6. If the Whistleblower decides to disclose his/her identity, his/her identification data will be processed on the basis of the Whistleblower's explicit consent (in accordance with Article 6(1)(a) of the GDPR).
7. In order to verify the report and take follow-up actions, the Company may collect and process personal data, including special category data, to the extent necessary to accept the report and take possible follow-up actions.
8. Personal data may be transferred by **the Company** to third parties such as:
    - External and/or legal advisors that **the Company** may turn to.
    - An external provider who manages the Ethics Line Platform dedicated to reports (for details, see the Information Clause at: NAVEX Privacy Statement | NAVEX

- competent authorities, when such an obligation arises from the provisions of law (e.g. for the purposes of explanatory proceedings conducted by public authorities or court proceedings).
- Other Takeda Group Companies.
- Third-party providers of services such as website hosting, provision of web technology and related infrastructure, and other similar services.

9. Personal data that is not relevant to the processing of the report will not be collected and will be deleted immediately in the event of accidental collection. Such personal data shall be erased within 14 days of establishing that they are irrelevant.
10. Personal data is processed for a period of 3 years after the end of the calendar year in which the follow-up actions were completed or after the end of the proceedings initiated by these actions.
12. **The Company** ensures the confidentiality of data in connection with the received report. **The Company** may transfer personal data to countries where other Takeda group entities operate or where **the Company** engages service providers. In cases where the transfer takes place to Third Countries that do not provide an adequate level of protection for personal data, **the Company** undertakes to put in place appropriate safeguards and to comply with applicable laws and regulations in connection with such transfer.

    In some cases, **the Company** undertakes to enter into contracts (e.g., the European Union Standard Contractual Clauses) or relies on other available data transfer mechanisms that are designed to provide adequate protection.
13. For additional information regarding the safeguards we have put in place to manage the cross-border transfer of personal information, please contact: privacyoffice@takeda.com.
14. Personal data will not be subject to profiling or automated decision-making.
15. Providing personal data is voluntary, but necessary for the proper receipt and consideration of the report made, in accordance with the **Company's** Internal Reporting Procedure and the provisions of the Whistleblower Protection Act.
16. The person who made the report has the right to request, within the limits set by the provisions of Chapter III of the GDPR: access to their personal data, including obtaining a copy of it, as well as rectification thereof. They also have the right to request deletion or restriction of processing, as well as to data portability.

17. To the extent that the data is processed on the basis of consent, the person who made the notification has the right to withdraw it at any time, without affecting the lawfulness of the processing carried out on the basis of consent before its withdrawal.
18. To the extent that the data is processed on the basis of the legitimate interest of **the Company**, the person who made the report has the right to object to the processing of their personal data, for reasons related to their particular situation, if the legitimate grounds for the processing of data by **the Company** do not override the interests, rights and freedoms of the person who made the report or **the Company** demonstrates the existence of grounds for establishing, pursuing or defending claims.
19. The person who made the report also has the right to lodge a complaint with the supervisory authority, i.e. the President of the Office for Personal Data Protection.
20. **The Company** has appointed, in accordance with Article 37 of the GDPR, a Data Protection Officer (DPO) who can be contacted at the following addresses:
    - privacyoffice@takeda.com. by email, or
    - by sending a message to the following address: IOD | Legal Department, Takeda Pharmaceuticals International AG, Thurgauerstrasse 130, CH-8152 Glattpark-Opfikon (Zurich), Switzerland.

Appendix 2: General authorization

……

(place, date)

AUTHORIZATION

(General)

receiving and verifying reports, follow-up, keeping a record of reports, processing personal data related to the report, confidentiality obligation, further authorisation, liability instruction

I, the undersigned, acting in accordance with the rules of representation at [*full name of the company*] (the "**Company**"), authorize [*name, surname, position*] to receive, verify and follow up on reports from whistleblowers and to maintain a register of internally reported breaches within the meaning of Article 27 and Article 29(2) of the Whistleblower Protection Act of 14 June 2024 (**the** "**Act**").

At the same time, I authorize you to process personal data related to the report, in particular whistleblowers, persons to whom the report relates and third parties indicated in the report, to the extent necessary to receive and verify reports and take follow-up actions.

In connection with this authorization, I oblige you to:

- maintain confidentiality and not disclose to unauthorised persons the information covered by the report and obtained in the course of proceedings related to it, in particular information on the basis of which the whistleblower, the person to whom the report relates and third parties named in the report can be identified, directly or indirectly, also after the expiry of the authorisation,
- protect the whistleblower, persons assisting in making the report and persons associated with the whistleblower from any form of retaliation,
- performing its tasks in accordance with the **Company's** Internal Reporting Procedure, **the Act** and the provisions of applicable law.

At the same time, I would like to inform and instruct you that, in accordance with **the Act**, the obligation to maintain the confidentiality of the identity of the whistleblower and other persons indicated above is reserved under the personal criminal liability.

On the basis of this authorization, the authorized person may grant further authorizations to take follow-up actions in relation to received reports.

This authorization is valid for the entire term of holding the position of **the Whistleblowing Officer** as described above. The authorization may be changed or revoked at any time.

……

(signature of person authorized to represent the Company)

STATEMENT

(of an authorised person)

I confirm that I have read this authorization**,** understand the rules and obligations arising from it and undertake to fully comply with its terms and perform my function in accordance with the **Company's** Internal Reporting Procedure, **the Act** and the provisions of applicable law.

……

(name, surname, date)

Appendix 3: Authorization for a specific case

……

(place, date)

AUTHORIZATION

(for a specific case)

follow-up, processing of personal data related to the report, confidentiality obligation, liability instruction

I, the undersigned, acting on the basis of the general authorization granted to me, authorize [*name, surname, position*] to participate in the process of taking follow-up actions in relation to the report of the breach[*individual report identifier*] (**the** "**Reported Breach**") in [*full name of the company*] (the "**Company**") within the meaning of Article 27 of the Whistleblower Protection Act of 14 June 2024 (the "Whistleblower Act").”). I declare that the general authorization granted to me has not been changed, revoked or expired.

At the same time, I authorize you to process personal data related to **the Reported Breach**, in particular the whistleblower, persons to whom **the Reported Breach** relates and third parties indicated in **the Reported Breach**, to the extent necessary to participate in the work of the explanatory committee in connection with **the Reported Breach**.

In connection with this authorization, I oblige you to:

- maintain confidentiality and not make available to unauthorised persons the information covered by **the Reported Breach** and obtained in the course of proceedings related to it, in particular information on the basis of which the whistleblower, the person to whom the Report relates and third parties indicated in the Report can be identified, directly or indirectly, also after the expiry of the authorisation,
- protect the whistleblower, persons assisting in making **the Reported Breach** and persons associated with the whistleblower from any form of retaliation,
- performing its tasks in accordance with the **Company's** Internal Reporting Procedure, **the Act** and the provisions of applicable law.

At the same time, I would like to inform and instruct you that, in accordance with **the Act**, the obligation to maintain the confidentiality of the identity of the whistleblower and other persons indicated above is reserved under pain of personal criminal liability.

This authorization is valid until the completion of the work of the explanatory committee in connection with the accepted **Application** or the expiration of the authorization on the basis of which it was issued. The authorization may be changed or revoked at any time.

……

(signature of a generally authorized person)

STATEMENT

(of an authorised person)

I confirm that I have read this authorization**,** understand the rules and obligations arising from it and undertake to fully comply with its terms and perform my function in accordance with the **Company's** Internal Reporting Procedure, **the Act** and the provisions of applicable law.

……

(name, surname, date)