INTERNAL REPORTING REGULATIONS

BEIERSDORF MANUFACTURING POZNAŃ SP. Z O.O.

1. PURPOSE AND SUBJECT OF THE REGULATIONS

1.1. The purpose of the Regulations is to define the internal procedures for reporting Breaches at Beiersdorf Manufacturing Poznań Sp. z o.o. (hereinafter referred to as ***the Company***) in case of Breaches reported directly by an Employee or a third party who are Whistleblowers using whistleblowing channels, thus in particular taking into account the requirements under Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and the Act; applicable data protection laws, as well as the need to safeguard confidentiality and integrity with respect to the Whistleblower and the person responsible for the Breaches.

1.2. The Company aims to maintain a Compliance Management System (CMS) that serves to prevent material compliance breaches and to ensure economic efficiency, respectively. The aim is to enable the identification of material areas of compliance risk at an early stage and to prevent and eliminate possible Breaches by establishing appropriate processes and measures. Given that Whistleblowers can play a vital role in identifying compliance violations, it is important to ensure that employees and third parties can confidentially report breaches of laws or internal regulations.

1.3. The Regulations define the rules for reporting Breaches and the rules for the Company's handling of Breach Reports regarding potential breaches of internal or external rules by the Company's Employees/representatives or business partners, and in particular specify:

a) types of Breaches that can be reported,

b) Whistleblowers and the method of protection of Whistleblowers,

c) the method of reporting Breaches,

d) procedure describing the rules for reporting Breaches

1.4. The Regulations apply only if the alleged breach is directly related to the Company's business;

1.5. Breaches disclosed in a manner other than through the Breach Reports are not covered by these Regulations;

1.6. The Whistleblowing Procedure described in the Regulation must be followed by any employee or representative of the Company designated to receive or follow up on reports of Breaches. If the Company engages external service providers to receive Breach Reports, the Company ensures that the service provider will also comply with the standards set out in these Regulations.

2. DEFINITIONS

2.1 **Breach** – an act or omission that is illegal or aimed at circumventing the law, concerning:

- corruption;
- public procurement;
- financial services, products, and markets;
- anti-money laundering and countering the financing of terrorism;
- product safety and compliance;
- transport safety;
- environmental protection;
- 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 computerised systems;
- financial interests of the State Treasury of the Republic of Poland, local government units, and the European Union;
- internal market of the European Union, including public-law rules of competition and state aid, and taxation of legal persons;
- constitutional human and citizen rights and freedoms – occurring in the relations of an individual with public authorities and not related to the areas indicated above, as well as:
- internal codes of conduct and procedures in force in the Company in the area of:
  - anti-corruption and conflict of interest;
  - standards of compliance with competition law.

2.2 **Whistleblower** – a natural person who reports information about Breaches obtained in a work-related context, including: employees; temporary employees; persons working on a different basis than an employment contract, in particular under a civil-law contract; entrepreneurs; company authorised representatives; shareholders or partners; members of a governing body of a legal person or an unincorporated legal entity; persons performing work under the supervision and management of a contractor, subcontractor, or supplier; trainees; volunteers; interns; and other persons indicated in Article 4 of The Whistleblower Protection Act of 14 June 2024 (Journal of

Laws 2024.928 of 2024.06.24) – hereinafter referred to as *the Act.*

Whistleblowers will also be persons who report information about a breach of the law in the work-related context before the employment relationship or other legal relationship constituting the basis for the provision of work or services or the performance of functions in or for a legal entity, or service in a legal entity or after their termination.

2.3 Corporate Compliance Management / Corporate Auditing – organizational units within the Beiersdorf Group (a group of capital companies in which Beiersdorf AG is the parent company and Beiersdorf Manufacturing Poznań Sp. z o.o. is one of the subsidiaries) dedicated to receiving Breach Report through the central contact channels indicated in the Regulations.

2.4 Report, Breach Report – the provision of information, including a reasonable suspicion of existing or potential Breaches, which have occurred or are likely to occur in the Company in which the Whistleblower participated in the recruitment process or other pre-contractual negotiations, works or worked, or in another legal entity with which the Whistleblower maintains or has maintained contact in a work-related context, or information regarding attempts to conceal such a violation of the law - using one of the reporting channels indicated in the Regulations.

2.5 Register – Register of Breach Reports

2.6 Retaliation – any direct or indirect action or omission in a employment context that is caused by a Report or public disclosure and that violates or is likely to violate the rights of the Whistleblower or causes or is likely to cause unreasonable harm to the Whistleblower, including the unjustified initiation of proceedings against the Whistleblower.

3. WHISTLEBLOWING

3.1. General

The Company offers the following channels, categories and technologies of Whistleblowing as indicated below to meet the diverse needs of different Whistleblowers. Whistleblowers can use centrally available channels (e.g. Reporting Hotline; Speak up. We care. Platform) and locally, allowing you to contact the Whistleblowing Officer.

3.2. Authorised to receive and hear reports

3.2.1. The entity authorized by the Company to receive Breach Reports is:

a) Corporate Compliance Management and Corporate Auditing Departments – with respect to Reports of Breaches reported in the central channel;

b) Whistleblowing Officer – a locally dedicated and independent person within the Company, authorized to receive Breaches Reports;

3.2.2. The entity authorized to take follow-up actions in connection with Breaches Reports made in the central and local channels is the Whistleblowing Officer.

3.2.3. The Whistleblowing Officer guarantees that the Follow-up is carried out impartially,

objectively and fairly, in accordance with the principle of confidentiality and respect for the rights of the Whistleblower and the person to whom the report relates.

3.2.4. The tasks of the Whistleblowing Officer include:

a) acceptance of the Report or confirmation of receipt of the Report submitted from the central channel,
b) initial verification of the Report;
c) timely confirmation of receipt of the report to the Whistleblower,
d) follow-up;
e) provide the Whistleblower with timely reply on the follow-up actions taken,
f) reporting to the Company's Management Board of any violations of the law,
g) recommending corrective actions to the Management Board,
h) keep a Register of Breach Reports.

3.3 Basic reporting channels

3.3.1. Center channel

A whistleblower may report a Breach:

a) in the form of **an e-mail**, to the following e-mail address: incidents_cases@beiersdorf.com or;
b) via **the Compliance hotline**: +49 40 4909-6050 , or;
c) through the **Speak up Platform. We care.** (available globally), including the "answering machine" module (VoiceIntake – for companies from the EU) available at: https://www.bkms-system.net/speakup.wecare

3.3.2. Local Channel

A whistleblower may report a Breach:

a) in the form of **an e-mail**, to the following e-mail address: SygnalistaBMP@Beiersdorf.com , or;
b) in the form **of a letter drawn up on paper**, to the postal address: Beiersdorf Manufacturing Poznań sp. z o.o., Whistleblowing Officer, 32 Gnieźnieńska Street, 61-021 Poznań, with the note "deliver in person", or;
c) **directly** through a meeting with the Whistleblowing Officer.

3.3.2. Alternative reporting channel

In order to ensure that Reports are handled in a fully objective and independent manner, the Company shall establish an alternative reporting channel, in the event that **the report relates to, for example, the Whistleblowing Officer or other person involved in the whistleblowing process**.

An alternative channel for submitting the Report may be sent to a selected Member of the Management Board in the form **of a letter drawn up on paper**, to the following postal address: Beiersdorf Manufacturing Poznań Sp. z o.o. Gnieźnieńska 32, 61-021 Poznań with the note "deliver in person";

In such a situation, the provisions of the Regulations apply accordingly – in particular, if the Report is not anonymous, the content of the Report or the identity of the Whistleblower shall not be disclosed to the persons concerned.

4. CONTENT OF THE REPORT

The Report should include:

a) personal data of the Whistleblower allowing for their identification and contact: name, surname and contact details;

b) indication of the name of the Company and the Department to which it relates;

c) a description of the Breach (what it concerns, when and where it took place or may take place),

d) indication of persons with knowledge of the Breaches – perpetrators, witnesses, victims, other persons with relevant information,

e) any documents (in any format) attached to the Report that may constitute evidence in the case,

f) any additional information that makes it probable that a Breach has occurred or justifies its suspicion or that may facilitate the clarification of the Report,

g) information whether the matter has already been reported in the past (e.g. to superiors or other persons in the Company).

The Report does not have to contain all the elements listed above, but their conclusion may facilitate the acceptance and consideration of the Report in the manner provided for in the Act and the Regulations.

5. ANONYMOUS REPORTING

5.1 The Company allows anonymous Reports. However, the Company points out that providing your personal data in the Report allows for faster clarification of the matter and more effective follow-up actions, while guaranteeing the confidentiality of the Whistleblower's identity.

5.2 If you wish to report anonymously, you are encouraged to use compliance incident reporting platform Speak up. We care. (referred to in point 3.1.1.c) above) and setting up a mailbox in accordance with the instructions described therein, enabling return contact.

5.3 If, however, in the course of handling an anonymous Report, the identity of the reporting person is disclosed or he/she confirms it himself/herself, such person becomes subject to protection as a Whistleblower within the meaning of these Regulations and is entitled to access to the reply.

6. WHISTLEBLOWERS PROTECTION

6.1 Protection and rights of the Whistleblower

Each Whistleblower is provided with:

a) Protection of their identity and confidentiality of the Report

b) Protection against Retaliation

c) the right to receive the reply with information about actions taken in relation to the Report.

6.2 Confidentiality of the report

All persons examining the Report shall keep their involvement in the process of handling the Report confidential, as well as all information obtained in connection with its course, including the identity of the Whistleblower and the person to whom the Report relates, as well as other personal data indicated in the Report.

Only persons with a written authorization from the Company may be allowed to receive and verify internal reports, take follow-up actions and process personal data of the persons referred to above. Authorised persons are obliged to maintain confidentiality with regard to information and personal data obtained as part of the receipt and verification of internal reports, and to take follow-up actions, also after the termination of the employment relationship or other legal relationship under which they performed this work.

Any data allowing the identification of the Whistleblower may be disclosed **only on the basis of his/her prior, explicit consent** – except for disclosure to competent authorities, when such an obligation arises from the provisions of law.

A breach of the duty of confidentiality may be the basis to legal and disciplinary liability of the person who committed such a breach.

6.3 Protection against Retaliation

It is forbidden to take Retaliate against the Whistleblower. This protection also covers persons assisting the Whistleblower in making a Report and other persons related to the Whistleblower, i.e. family, relatives and relatives.
The Company also prohibits Retaliation against a legal entity that is owned by the Whistleblower, for which Whistleblower worked for or with which the Whistleblower is otherwise associated.
Any Whistleblower who experiences or who knows of any Retaliation should immediately report it on the same terms as reporting Breaches.

7. PROCEDURE FOR CONSIDERING THE REPORT

7.1 Initial verification of the Report

The Whistleblowing Officer conducts a preliminary verification of the Report:

a) makes sure that the Report contains all the information necessary to process it. If they notice significant deficiencies, they contact the Whistleblower, unless the Report was submitted anonymously or the Whistleblower did not allow contact with them;
b) determines whether the reported case may constitute an Breach within the meaning of the Regulations;
c) assesses how serious the consequences of the reported Breach may be from the point of view of the interests of the Company and the Company's Employees.

7.2 Acknowledgment of receipt of the Report

The Whistleblowing Officer shall inform the Whistleblower of receipt of the Report no later than **within 7 days** of its receipt, unless the Whistleblower has not provided a contact method to which the confirmation should be submitted.

7.3 Proceedings in individual cases of Employees

If the Report concerns individual violations of the rights and interests of the Employee that do not constitute Breaches (e.g. cases in the area of labour law, mobbing, discrimination), the Whistleblowing Officer:

a) informs the applicant that such a notification does not fall within the scope of these Regulations, and
b) instructs the applicant about the possibility of making a report directly to the HR Department.

This excludes further proceedings of the case under the rules described in these Regulations, and the status of a Whistleblower is not granted to the person making such a report.

8. CONTENT OF THE REPLY TO WHISTLEBLOWERS

The Whistleblowing Officer provides the reply to the Whistleblower (unless the Whistleblower has not provided a contact address to which the reply should be provided). The reply is provided within **3 months** from the date of confirmation of receipt of the Report or, in the event of failure to provide the confirmation referred to in point 6.2 – 3 months from the expity of 7 days from the date of submission of the Report.

The content of the reply should include information about the planned or taken follow-up actions and the reasons for such actions.

9. INVESTIGATION

9.1 Initial analysis of the Report

If, as a result of the initial verification of the Report, the Whistleblowing Officer finds that the Report concerns the categories of violations indicated in point 2.1 of the Regulations, the Whistleblowing Officer shall immediately initiate an explanatory proceeding aimed at a thorough assessment of the veracity of the allegations contained in the Report.

9.2 Appointment of persons to help clarify the Report

The Whistleblowing Officer may set up a Report investigation team of people with relevant knowledge and experience who can help resolve the Report efficiently. Such persons may be both employees of the Company and external advisors.
In selecting such persons, the Whistleblowing Officer ensures that they **are impartial and that there is no potential conflict of interest in connection with the case**. Before being admitted to the case, each such person **must sign an appropriate statement** obliging them to maintain the confidentiality of the information related to the Report.

9.3 Investigation

The Whistleblowing Officer takes action to clarify the matter, e.g.:

a) request additional information from the Whistleblower;
b) receive explanations from the Whistleblower or the person to whom the Report relates and another person who may have information relevant to the clarification of the Report;
c) request information, explanations or documents from all organizational departments of the Company;
d) view documents, data, records in the IT system, monitoring recordings, GPS and other records of data and information;
e) secure devices that are data carriers, such as computers, laptops, phones, tablets;
f) obtain opinions of experts and external experts,
g) apply to the Management Board of the Company for the application of protective measures, such as suspension from performing functions, removal from performing specific tasks.

All activities undertaken as part of the investigation are confidential and all members of the investigation team are obliged to maintain confidentiality.

9.4 Corrective actions under the follow-up

If justified by the outcome of the investigation, the Whistleblowing Officer develops a corrective action plan (or has it developed) and submits it to the appropriate person(s) or organizational unit for implementation. If the proposed corrective actions require a decision of the Company's Management Board, the Whistleblowing Officer submits a corrective action plan for approval by the Management Board, subject to the confidentiality requirements described in these Regulations.

Corrective actions include all actions aimed at eliminating the Breach and its

consequences, including minimizing the legal, financial and image risk for the Company and the Group. These can be activities consisting of, for example:

a) initiation of disciplinary proceedings or other appropriate proceedings against the person who committed the Breach,

b) modification of the applicable procedures to prevent the recurrence of similar Breaches in the future,

c) carrying out additional education or training activities;

d) increasing the frequency of audits of a given area,

e) carrying out structural changes or transferring competences,

f) taking appropriate legal measures, including procedural ones.

The action plan should define specific tasks, assign responsibility for their performance to specific Employees or Departments and specify the deadline for the implementation of tasks.

9.5 Documenting the proceedings

All activities important from the point of view of a reliable explanation of the case **should be documented** (reports, data summaries, e-mail correspondence, notes from interviews, notes from meetings of the investigation team, etc.). All documents related to activities of the proceedings are strictly confidential, and the persons who create such documents, after submitting them to the Register and closing the case, are obliged to permanently remove such documentation from their resources.

10. REGISTER KEEPING

10.1 The Register records each Report, submitted under the terms and using the channels described in the Regulations;

10.2 The Register includes:

a) Report number;

b) description of the Breach;

c) personal data of the whistleblower and of the reported person (necessary to identify these persons);

d) whistleblower's contact address;

e) date of submitting the Report;

f) information on follow-up actions;

g) Report completion date.

10.3 The Register is kept in electronic form by the Whistleblowing Officer on the basis of

an appropriate authorization from the Company. They ensure the confidentiality and security of data stored in the Register and, as a rule, have exclusive access to them.

10.4 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 the follow-up actions were completed or after the end of the proceedings initiated by these actions.

11. EXTERNAL REPORTS

Whistleblowers have **the right to report certain breaches of the law, listed in the Act, to the Ombudsman or to the public authority responsible for the category of Breaches in question**, and, where appropriate, to the institutions, bodies, offices or agencies of the European Union, without following the procedure provided for in these Rules of Procedure, without first making an internal report.

12. RESPONSIBILITY

Reporting in bad faith – if the Report is made in bad faith, i.e. in a situation where the person reporting the alleged violation of the law referred to in point 2.1 indents 1-17 of the Regulations knows that no violation of the law has occurred, then such a person is subject to criminal liability.

13. FINAL PROVISIONS

1. Knowledge of the rules set out in the Regulations is the responsibility of all employees of the Company;
2. The employee is familiarized with the provisions of the Regulations before he or she is allowed to work.
3. The Internal Reporting Regulations enter into force after 7 days from the date of announcement to the Employees in the manner provided for by the Employer.

Attachments:

Appendix No. 1 - Information clause regarding the processing of personal data

Appendix No. 1

Information clause regarding the processing of personal data

Pursuant to Article 13 of the General Data Protection Regulation of 27 April 2016 (hereinafter referred to as the "GDPR"), we provide you with information on the principles of processing your personal data by Beiersdorf Manufacturing Poznań sp. z o.o., as well as on your rights.

Who is the administrator of personal data?

The administrator of personal data is Beiersdorf Manufacturing Poznań sp. z o.o. with its registered office in Poznań, 61-021 Poznań, Gnieźnieńska 32 (hereinafter referred to as: Beiersdorf or the Administrator).

Contact details of the Data Protection Officer.

The Controller has appointed a Data Protection Officer who can be contacted via email ido@beiersdorf.com in all matters related to the processing of personal data and the exercise of rights related to data processing.

For what purpose and on what basis do we process data?

The information provided in this document relates to the persons who are the Whistleblower, the persons to whom the Report relates, employees and other persons, contained in the Report for purposes related to the reported cases of Infringement, on the basis of:

a. consent (in accordance with Article 6(1)(a) of the GDPR), if the Whistleblower has expressly consented to the disclosure of the Whistleblower's identity;

b. a legal obligation under the provisions of the Act on the Protection of Persons Reporting Breaches of Law (in accordance with Article 6(1)(c) of the GDPR) in connection with the provisions of the Act of 14 June 2024 on the Protection of Whistleblowers, in order to perform tasks related to handling reports;

c. the legitimate interest of the controller, which is receiving, verifying and clarifying reports, counteracting Infringements in the Company, as well as establishing or defending against claims (in accordance with Article 6(1)(f) of the GDPR). The Company may , in order to verify the Report and take follow-up actions, collect and process personal data of the person to whom the Report relates, even without their consent.

Data recipients

The recipients of the data may be entities entrusted with the processing of personal data on behalf of and on behalf of Beiersdorf . Such recipients may be entities from the Beiersdorf Group, entities providing and supporting IT systems used by Beiersdorf and entities providing services in connection with the received Report (e.g. legal services). In addition, Beiersdorf will share personal data with other recipients insofar as such an obligation arises from legal provisions.

The Company ensures the confidentiality of data in connection with the received Report.

The Company may transfer personal data to entities authorized to do so under the law. In addition, the Company will provide personal data to the Whistleblowing Officer and other persons authorized to clarify the Report.

Personal data will not be transferred to a third country or an international organization. Personal data will not be subject to profiling or automated decision-making.

In the course of the proceedings, it may be necessary to forward the Notification to other employees of the Controller or to employees of other companies of the Beiersdorf AG group (e.g. if the Notification relates to processes in a subsidiary of Beiersdorf AG). These companies may be based outside the European Union or the European Economic Area and different data protection laws may apply there. In this case, we ensure that the data is transferred in accordance with the applicable data protection laws. Depending on where you want to transfer your data, we agree on standard data protection clauses, apply internal data protection rules, or only transfer data to companies that comply with the EU-US Privacy Framework or are based in countries for which the European Commission has issued an adequacy decision. In addition, we always act in accordance with the applicable data protection law when processing applications.

Using the whistleblowing system

Communication between the whistleblower's computer and the whistleblowing system is encrypted (SSL). When you use the system, your computer's IP is not saved. In order to maintain the connection between the computer and the BKMS® System (Speak up. We Care), a cookie is stored on your computer's hard drive. A cookie only contains a session ID and is only valid until the end of the session, i.e. it expires when you log out or close your browser.

However, keep in mind that your computer may show traces of using the ticketing system. If you are using the system on a company computer, think about deleting the cache and browser history later. If your browser allows you to use the Internet in private mode, use it so you don't have to manually delete your data.

You can also create a secure mailbox with a nickname/username and password of your choice. It allows you to anonymously and securely send reports to the person conducting the proceedings. The data is stored exclusively within the whistleblowing system and is specially protected during the process; This works differently than in the case of standard email communication.

Send attachments

When sending a report or additional information to the person responsible in accordance with the Regulations, you can also send attachments. If you want to submit a report anonymously, please note: Files may contain hidden personal information, which puts your anonymity at risk. Before sending the file, delete such information. If you can't remove this information, or if you're not sure how to do it, copy and paste the file into the body of your report, or send a printed copy of the document anonymously to the investigator.

How long will we process the data?

Personal data and other information contained in the register of internal reports are stored for the period specified in clause 10.4 of the Regulations.

What are your rights?

You have the right to:

a) withdraw your consent at any time. The withdrawal of consent does not affect the lawfulness of the processing carried out before its withdrawal. If you withdraw your consent to disclose your identity, your personal data will not be shared (from the moment you withdraw your consent).

b) access their personal data and receive a copy of the personal data subject to processing;

c) rectify their incorrect data;

d) request the deletion of data (the right to be forgotten) in the event of a request the circumstances provided for in Article 17 of the GDPR;

d) request restriction of data processing in the cases indicated in Article 18 of the GDPR;

e) object to the processing of data, but it is entitled 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 (in the cases referred to in Article 21 of the GDPR);

f) data portability.

If you believe that your personal data is processed unlawfully, you may lodge a complaint with the supervisory authority (UODO, 2 Stawki Street, Warsaw).

If you have any questions regarding the manner and scope of the processing of your personal data within the scope of the Administrator's activities, as well as your rights, you can contact us at the following address: ido@beiersdorf.com or in writing to the Administrator's address.