Whistleblower Policy

Annex 2

Effective date:
31.07.2024.

Data Protection Notice

1. Purpose of this data protection notice

(1) This Data Protection Notice applies to every member of the OBO-Group (hereinafter referred to as: Group-Companies), as to their employees and members of managing bodies and other individuals concerned by a report, when involved in the handling or investigation of a report submitted to OBO Bettermann Holding GmbH & Co. KG with registered office at Hüingser Ring 52, 58710 Menden (Sauerland), Germany, [Reg. number: HRA 4854, VAT number: DE811792270] and/or OBO Hungary Kft. with registered office at Alsóráda 2, 2347 Bugyi, Hungary, [Reg. number: 13-09-096185, VAT number: HU10847392] as described under Annex 1. All Group-Companies involved in the processing of the personal data concerned by each report shall be considered as joint controllers.

(2) The Data Protection Notice of the OBO-Group can be accessed at any time at this link.

(3) The OBO-Group is committed to protect the personal data of whistleblowers, other persons covered by this Whistleblower Policy and any individuals mentioned in or concerned by a report and attaches the utmost importance to respecting their right to informational self-determination. The OBO-Group shall treat personal data confidentially and shall take all technical and organisational measures to ensure the security of the data.

2. Name and address of the data controller(s)

(1) The primary responsible party for the purposes of data protection law is the Group-Company concerned with the report as listed under Annex 3, together with or independently of other Group-Companies concerned, as the case may be (hereinafter "we", "us", "our", "controller(s)"):

- When reporting with the competent office in Germany the controller is**: OBO Bettermann Holding GmbH & Co. KG**
  Hüingser Ring 52
  58710 Menden,
  Germany

Telephone: +49 (0)2373 89-0
Fax: +49 (0)2373 89-238
E-mail: info@obo.de
[Reg. number: HRA 4854, VAT number: DE811792270] or

- When reporting with the competent office in Hungary the controller is: **OBO BETTERMANN Hungary Kft.**
  H-2347 Bugyi, Alsóráda str. 2.,
  Hungary
  E-Mail: compliance@obo.de
  Telefon: +0036 29 349-708
  [Reg. number: 13-09-096185, VAT number: HU10847392]

(2) Contact data of the data protection officer

OBO Bettermann Holding GmbH & Co. KG
Josef Honert
- Data Protection Officer -
Hüingser Ring 52
58710 Menden
Germany
Tel.: +49 (0)2373 89-1351
E-mail: datenschutz@obo.de

(3) The office for processing your personal data at the Ombudsperson is:

DR. WEHBERG & PARTNER mbB
Auditors, tax consultants and lawyers
Feithstraße 177, 58097 Hagen, Germany
Telephone: +49-(0)2331-1098-1234
E-mail: obo-hinweise@wehberg.de

Contact person for data protection at DR. WEHBERG & PARTNER mbB is:

DR. WEHBERG & PARTNER mbB
- the Data Protection Supervisor -
Feithstraße 177, 58097 Hagen, Germany
E-mail: datenschutz@wehberg.de

Further information can be found on the following Internet pages https://wehberg.de/impressum and https://wehberg.de/datenschutzerklaerung.

3. Processing of personal data

Personal data means any information relating to an identified or identifiable natural person, such as names, addresses, telephone numbers, e-mail addresses, contract master data, contract accounting data and payment data, to the extent that they are an expression of the identity of a natural person. We only process personal data if there is a legal basis to do so.

Automated decision-making, including profiling, does not take place in connection with the use of the whistleblowing system of the OBO-Group.

4. Categories of data processed

(1) The use of the OBO-Group's whistleblowing systems for a report is voluntary. If you use the system, we will ask you to provide information on the following categories of data

- Communication data (e.g. name, telephone, e-mail, address)
- Employee data of OBO-employees and
- If applicable, names and other personal data of the reporting persons, the persons mentioned in a report, and the persons involved in (and the persons identified in connection with) the processing of the facts reported and further investigation thereof.

(2) If you answer all the questions in the report in full, this will help the controller(s) to process your report. If you provide incomplete information, or decide to stay anonymous, we may not be able to process your report or may be delayed in doing so.

(3) We may collect and process the following categories of personal data through the use of the whistleblowing system of the OBO-Group:

- breaches and related facts reported (including data relating to fraud or allegations of fraud, or other violations of the law, or relating to suspected or possible criminal offences only to the extent permitted under applicable law, for example, in order for the affected Group-Company to manage its own litigation), communications and information collected/reviewed in connection with the reporting and investigation of the facts reported (subject to applicable requirements under applicable law), and investigation report;
- consequences of the investigation, including possible disciplinary measures as well as criminal allegations, prosecutions or convictions, as the case may be;
- protection of the relevant persons against retaliation;
- follow-up on the report.

Sensitive personal data and personal data relating to suspicions, prosecutions or convictions of criminal offences shall only be processed as permitted under applicable data protection laws.

The source from which personal data originates is typically from the individual to whom it relates (e.g. employees themselves) and personal data that we receive in a permissible manner from publicly available sources and/or from third parties as further described below.

We may collect personal data in the ways listed below:

- Collection of personal data directly from the data subject, such as through a report or other forms or information data subjects provide us in connection with their employment;
- Collection of personal data during data subjects' activities in the course of their employment, such as through their performance and interaction with other employees, customers, or other individuals; and
- Collection of personal data from other parties such as reporting persons and other employees.

5. Purpose of processing and legal basis

(1) The purpose of the whistleblowing system of the OBO-Group is to provide a communication channel for your report and to ensure that your report is handled by the OBO-Group in accordance with the processes of the compliance management system as an implementation of the requirements of company law.

(2) In particular, your personal data will be processed for the following purposes

- Compliance reporting: Indication and follow-up of reports concerning a possible violation of compliance requirements. You may report such violations with your name or anonymously.

  Legal basis: The processing activities are carried out based on a legal obligation to which the Group-Companies are subject (Art. 6 (1) (c) of the GDPR), as provided by the applicable regulations regarding whistleblowing.

  In countries where there is no legal obligation to establish a whistleblowing system the processing activities are carried out based on the legitimate interest of the controller(s) (Art. 6 (1) (f) GDPR) in the prosecution of criminal offences, the enforcement of civil claims, the further development or termination of an employment relationship or the detection of criminal offences in connection with the employment relationship.

- Compliance Management: Central administration and allocation of Group-wide compliance issues.

  Legal basis: Legitimate interest of the controller(s) in obtaining a central overview of reports as part of the governance function (Art. 6 (1) f) GDPR) and for the exercise and defense of our rights.

  In exceptional circumstances, such as when we intend to disclose the reporting person's identity to third parties, we may process personal data on the basis of the data subject's explicit consent.

If a report contains special categories of personal data, such data shall only be processed

(i) if the processing is necessary for the performance of obligations and the exercise of specific rights of the controller(s) or the data subject in the field of labour law and social security and social protection law, to the extent permitted by EU or national law or by a collective agreement under national law providing adequate safeguards for the fundamental rights and interests of the data subject (Art. 9 (2) (b) GDPR), or

(ii) if the processing is necessary for the establishment, exercise or defence of legal claims (Art. 9 (2) (f) GDPR). If special categories of personal data are included in a report but are not clearly relevant to the reported matter, they will be deleted immediately and securely.

Personal data relating to suspicions, prosecutions or convictions of criminal offenses shall only be processed as specifically authorized by EU or national law.

6. Transfer of data to OBO-employees, potentially suspected persons and to other data controller(s)

(1) When processing a report, it is necessary to forward the report, in whole or in part, to the OBO-Group employees responsible for processing it and to the employees of the Group-Companies affected by the report. Your information will only be available to those employees who have a need to know in order to process your report.

(2) The right of the suspected person to be informed about the processing of his personal data may be limited or delayed. It may be limited by existing national legislation (Art. 23 GDPR) or, in the absence of such legislation, it may be delayed in exceptional circumstances, for example in case of risk of destruction of evidence, or when it is likely to seriously jeopardize the purpose for which information is being processed.

(3) Your personal data will only be transferred to the affected Group-Company to the extent necessary to comply with further legal obligations. In addition, data may be transferred to other controllers (e.g. authorities) if we are required to do so by law or by enforceable orders of authorities or courts.

7. Transfer to recipients outside the EU and/or the EEA

Controller(s) may only transfer personal data from the EU/EEA to third parties outside the EU/EEA (including granting access from a third country) if

- the third country offers an adequate level of data protection recognised by the EU Commission and the respective country, or
- the transfer is subject to EU standard contractual clauses. It is the responsibility of the controller(s), with the assistance of the third party if necessary, to assess whether the level of protection required by EU law is respected in the third country in order to determine whether the guarantees provided by the EU standard contractual clauses can be met in

practice. If not, the third party must take additional measures to ensure a level of protection substantially equivalent to that in the EU/EEA, or

- exceptionally (i.e., only if the above measures cannot be implemented), an exemption for specific situations applies (e.g., the transfer is necessary for the establishment, exercise or defense of legal claims).

A copy of the relevant safeguards for the transfer of your personal data outside the EEA can be obtained by contacting us using the contact details referred to in Section 2 above.

8. Duration of storage; Retention periods

(1) In principle, we will keep your data for as long as is necessary to investigate the compliance incident that is the subject of your report. After all work relating to the report has been completed, we will delete your personal data, except for data that needs to be retained and processed in order to exercise and defend our rights.

(2) When we delete personal data that we retain and process to exercise and defend our rights will depend on the expiry of the maximum limitation period for regulatory and criminal offences or for the enforcement of civil claims.

(3) The above is without prejudice to specific data retention periods applicable in certain jurisdictions, as set out in the national legislation listed in Annex 3, which shall prevail in case of conflict.

9. Security

(1) Our employees and service providers are required to keep our information confidential and to comply with applicable data protection laws.

(2) All incoming reports are received by a small number of authorized and specially trained OBO-Group employees and are always treated confidentially. The OBO-Group employees will review the facts and conduct any further investigation required by the specific case. All such persons who have access to the data are required to maintain confidentiality.

10. Right of information and access

You have the right to obtain information from the controller(s) as to whether or not your data is being processed and, if so, to access your personal data that we are processing.

11. Right to rectification

You have the right to correct or supplement personal data if they are incorrect or incomplete.

12. Right to erasure

You have the right to request erasure of personal data concerning you in the specific circumstances laid down in applicable data protection law (e.g., the GDPR). Existing retention periods and interests worthy of protection that prohibit deletion must be observed.

13. Restriction of processing

You have the right to restriction of processing of your data if you dispute its accuracy or if the controller(s) no longer need(s) the data while you need the data for your legal claims. You can also request that the controller(s) restrict(s) the processing of your data if it would otherwise have to delete the data or if it is reviewing an objection by you.

14. Data portability

You have the right to receive personal data concerning you, which you have provided, in a structured, commonly used and machine-readable format and may have the right to transmit that data to another entity.

15. Objection to data processing

You also have the right at any time to object to the processing of your data by the controller(s) on grounds relating to your particular situation, provided that the processing is carried out on the legal basis of „legitimate interest". We will then stop processing your data unless we can demonstrate - in accordance with the legal requirements - compelling legitimate grounds for further processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims (Article 21 GDPR).

16. Right to withdraw consent

Where the processing of personal data is based on your consent, you may withdraw your consent at any time. Such a withdrawal will not affect the lawfulness of the processing prior to withdrawal of the consent.

17. Right to complain to a supervisory authority

You have the right to complain to a data protection authority. You can contact the data protection authority responsible for your place of residence or your country, place of work or for the place of an alleged infringement of the GDPR. A list and contact details of the data protection authorities can be found in Annex 3. The list of EU national data protection authorities is available at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

18. Changes to the Data Protection Notice

We reserve the right to change our security and privacy practices. If we do, we will update our privacy notice and, to the extent required by applicable law, inform you accordingly.