

## Privacy Statement for the submission of information

---

Updated: 17.11.2023

### Data protection is important to us

---

As a public company, OeBB attaches great importance to the protection of data privacy. This is especially relevant for the handling of notices regarding unlawful and other non-compliant behaviour.

In order to give everyone the opportunity to submit relevant information, OeBB has not only set up the e-mail address [compliance@oebb.at](mailto:compliance@oebb.at), but also provides a web platform. This web platform is provided for OeBB by a well-known external provider of IT solutions in the compliance area.

This privacy statement shall make transparent how data received at this e-mail-address and web platform and other data collected in connection with such information will be used.

### General Data Protection Regulation

---

Articles cited in this document refer to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as "GDPR"). The GDPR is directly applicable in all EU Member States.

### Whistleblower Protection Act

---

The Austrian Whistleblower Protection Act and corresponding legal acts in national legal systems (HSchG) implement the EU Whistleblowing Directive 2019/1937 into national law. Companies are obliged to provide reporting channels to enable whistleblowers to report concerns about violations confidentially. Whistleblowers are granted special protection by the HSchG. References to specific paragraphs and text passages refer to the Austrian HSchG.

### Controller

---

Controller for personal data processed in the course of the whistleblowing (e.g. the person of the whistleblower or of persons who could be involved in the legal violations outlined) as defined in Art. 4 item 7 of the GDPR is every OeBB group company to the detriment of which the investigated act was committed or the right of which is encroached upon by the investigated act. This also applies if the company is not expressly mentioned or incorrectly named in the information received.

The OeBB Group companies collectively operate the whistleblower system pursuant to § 8 line 4 HSchG and have concluded an agreement as "joint controllers" pursuant to Art 26 GDPR. This joint responsibility only includes receiving information and fulfilling the disclosure obligations prescribed in § 13 line 9 HSchG.

The Compliance Office of ÖBB-Holding AG, Am Hauptbahnhof 2, 1100 Vienna (Compliance Office) constitutes the internal organisation as defined by § 5 line 6 HSchG.

### Initiation of investigations

---

The information received at the e-mail address [compliance@oebb.at](mailto:compliance@oebb.at), via the web platform or by other means (e.g. by post or telephone) is first reviewed for plausibility. The information is then forwarded to the relevant Group company. Each Group company is responsible for its business area to ensure that the suspicion on which the information is based is investigated.

That Group Company is also the "master of the data" that is determined in the course of the investigation - and is thus the "controller" within the meaning of the GDPR.

A link to the most important OeBB Group Companies and their imprints is available at: <https://konzern.oebb.at/en/imprint>. The imprints also show the respective corporate purpose of the Group Companies.

### Group wide processors

---

In the analysis of the information received, the Group Companies are supported by the Compliance Office of ÖBB-Holding AG, which is headed by the Chief Compliance Officer of OeBB.

ÖBB-Holding AG therefore participates in the analysis of the incoming information as a "processor" in the sense of Art 4 item 8 GDPR. The Compliance Office assigns the incoming information to the Group Company concerned and supports the company in the internal investigation and the related documentation.

The web platform used to receive reports is provided for OeBB by the company EQS Group AG (formerly Business Keeper GmbH), D-80333 München. It is technically impossible for EQS Group AG itself to have access to the data transmitted via the web platform or to access the information stored there. EQS Group AG is therefore not a processor within the meaning of Art. 4 line 8 DSGVO.

### Data protection officer

---

Within OeBB Group, a data protection officer has been appointed for each Group Company. Please find an overview at: <https://konzern.oebb.at/en/imprint/data-protection-officers>.

The Group's data protection officer is also available at the e-mail address [datenschutz.konzern@oebb.at](mailto:datenschutz.konzern@oebb.at).

### Legal basis for data processing

---

The legal basis for data processing is

- Art 6 par 1 lit a GDPR, i.e. the consent given by the whistleblower for the processing of their data,
- Article 6 par 1 lit c GDPR, i.e. the legal obligation arising from the HSchG for the controller (the relevant OeBB Group company) to set up channels for reporting legal violations and to document and investigate the reports received,
- Art 6 par 1 lit f GDPR, i.e. the legitimate interests pursued by the controller (the relevant OeBB Group company), to investigate indications of misconduct to the detriment of the company.

If the use of data is based on the consent of the whistleblower, the withdrawal of this consent does not affect the legality of the processing and transmission of the data carried out on the basis of the consent until the withdrawal (Article 8 par 2 and par 4 HSchG). Once information has been provided, it can therefore not be withdrawn or "revoked".

### Description and scope of data processing

---

The purpose of the processing activity is to investigate facts

1. which involve a breach of Union law in the areas referred to in Art 2 of Directive (EU) 2019/1937 of 23 October 2019 and the corresponding national implementing provisions (HSchG); or
2. that are otherwise likely to give rise to suspicion of misconduct,

- which falls within the competence of the Compliance Office according to OeBB Group Guideline 15 or
- serves to avert severe disadvantages for the controller resulting from misconduct of its employees due to other unlawful conduct.

### Anonymity of the whistleblower

---

In general, the identity of the whistleblower will only be disclosed upon consent. On the web platform, whistleblowers can submit tips anonymously and subsequently also communicate anonymously with employees of the Compliance Office.

If the identity of the whistleblower is known to the Compliance Office, it will be disclosed in these cases regardless of the whistleblower's consent:

- There is an obligation under public law to disclose the identity of the whistleblower to a court or administrative authority, e.g. when a witness is interrogated (OeBB Group employees dealing with compliance matters are subject to the obligation to testify and have no right to refuse to testify)
- Information provided to data subjects in accordance with Art 15 GDPR, if the notice is untrue and has been given in bad faith and therefore the whistleblower has no legitimate interest in keeping his or her identity secret.

### Notification of data subjects

---

If information provided by a whistleblower mentions a specific person (in particular in connection with a suspicion directed against him or her), the data will be stored in connection with the information, and the data subject will be informed of the data storage in accordance with Art 14 GDPR immediately, as soon as this information can no longer jeopardise the purposes of the investigation.

As a matter of principle, this takes place during the internal investigation while the respective person is being interviewed by the Compliance Office, since prior notification could jeopardise the purpose of the investigation.

The data subject will be informed about the investigated suspicion in due course. Likewise, the OeBB Group Company responsible for investigating the suspected case as well as any other OeBB Group Companies involved will be informed. In addition, the manner in which rights of defence and other information rights can be exercised will be provided.

### Dealing with other information

---

Information received that is not necessary for the pursuit of the purpose outlined above, i.e. that does not relate, for example, to misconduct of an employee or a company body of an OeBB company or that relates to conduct that can obviously neither have caused OeBB any damages or other disadvantages nor violate Union law, will not be pursued by Compliance and, if appropriate, forwarded to the relevant internal departments.

However, OeBB reserves the right to forward certain information to public authorities, which upon first impression indicate an incident that is not compliance-relevant, but relevant under criminal law, while maintaining the anonymity of the person who has provided information in the sense described above.

### Data recipients

---

- OeBB-internal recipients  
Personal data is used for reporting to the responsible executive management body, which ultimately decides on the further procedure (e.g. disciplinary consequences).

Data is also used for reporting on the measures taken within OeBB Group to executive bodies of the subgroup's parent companies as well as ÖBB-Holding AG.

- External recipients

Data determined as part of the processing of information can be transmitted to security authorities, regulators, public prosecutors' offices and criminal courts for the purposes of criminal prosecution in order to provide evidence in criminal matters if required. Data may also be used in civil court proceedings to enforce claims and to provide evidence. The intervening OeBB company may appoint professional party representatives (lawyers) to represent it in the respective proceedings.

In such cases, the identity of the person who has provided information is only revealed upon consent or if an official act mandates disclosure. In this context, please be aware that employees of OeBB Group who are involved in compliance matters are subject to the duty to testify and have no right of refusal to testify.

### Service provider

---

In addition to the web platform for case management, ÖBB-Holding AG uses a software application operated by ÖBB-BCC GmbH as a processor.

In individual cases, ÖBB-Holding AG uses forensic service providers, whose activities are protected by an obligation of professional secrecy, as additional processors for the investigation of complex facts.

Corresponding agreements are concluded with all processors. In any case, processors are prohibited from deciding on the use of data.

### Storage period

---

Data gathered within the investigation is stored for five years. In addition, data is stored for as long as it is required to carry out administrative or judicial proceedings that have already been initiated or investigative proceedings under the StPO (§ 8 line 11 HSchG). If shorter periods are required according to applicable national legislation, these will be considered accordingly.

Information relating to the case, especially interview transcripts, notes and copies of other files are archived electronically after this storage period has expired. Archiving is performed in a way so that OeBB's employees and company bodies cannot access such archived files anymore. Access is then only possible for the Chief Compliance Officer, who is not subject to any instructions from the corporate bodies regarding his activities and only acts upon official request. Processing operations that are carried out are logged. Log data on these processes will be deleted three years after the retention obligation ceases to apply (§ 8 line 11 HSchG).

The data will be completely deleted after seven years.

Unsubstantiated reports not within the scope of the HSchG are archived two months after completion of the investigations.

### Rights of data subjects

---

You have the following rights with regard to the use of your personal data:

- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

In case you want to exercise the aforementioned rights against ÖBB-Holding AG or any other Group Company, please send a message to the above-named contact details or to the data protection officer mentioned in each subsidiaries' imprint. Please indicate in the subject field the assertion of your rights in accordance with the GDPR as well as the context of your question (data processing in the context of a specific compliance case).

Please be aware that a compliance investigation is not based on consent and there is thus no right to data portability.

You have the option of lodging a complaint with a data protection supervisory authority. The supervisory authority responsible for OeBB Group is: Austrian Data Protection Authority (Österreichische Datenschutzbehörde), Barichgasse 40-42, 1030 Vienna; e-mail: [dsb@dsb.gv.at](mailto:dsb@dsb.gv.at).