TRANSLATION FROM THE GERMAN LANGUAGE

Data protection information on the whistleblowing system

1. Controllers

Controllers within the meaning of the GDPR for data processing in connection with the whistleblower system are as joint controllers pursuant to Art. 26 GDPR:

- The **Whistleblowing Officer (Germany/Austria)**
  Stella Grenz-Richter, Potsdamer Straße 6, 64832 Babenhausen

- The **Whistleblowing Officer (Poland)**
  Slawomir Maciag, ul. Jana Pawła II 66, 05-500 Piaseczno, Poland

- The **Whistleblowing Officer (Romania)**
  Elena Poiana, Soseaua de Centura 28-35, Chiajna, Ilfov 077040, Romania

  and

- the respective **Logwin group company(ies)** to which the information relates and which are involved in the further processing of the information ("Logwin"). The following companies have a whistleblowing office:

  Logwin Solutions Logistik GmbH
  Logwin Holding Aschaffenburg GmbH
  Logwin Air + Ocean Deutschland GmbH
  Logwin Air + Ocean Austria GmbH
  Logwin Solutions Austria GmbH
  Logwin Poland Sp.z.o.o (PL)
  Logwin Romania S.R.L. (RO)

  You can contact the data protection officer of the German Logwin Group companies under:
  Data Protection Officer
  c/o Logwin Holding Aschaffenburg GmbH
  Stockstädter Straße 12, 63762 Großostheim, Germany
  E-Mail: dataprivacy@logwin-logistics.com

  For the Austrian Logwin Group company(ies) there is currently no requirement by national law to appoint a data protection officer. If you have any questions regarding data protection you can also contact dataprivacy@logwin-logistics.com.

  You can contact the data protection officer of Poland under:
  slawomir.maciag@logwin-logistics.com

  For the Romanian Group company there is currently no requirement by national law to appoint a data protection officer.

The respective data processing operations, responsibilities and competences of the Whistleblowing Officer and Logwin are described below in section 2 (Art. 26 (2) GDPR).

2. Type and scope of data processing

a) The Whistleblowing Officer receives information via the reporting channels described in the "Guideline on the Use of a Whistleblowing System" (in particular by email and by telephone).

They first check whether the whistleblower belongs to the group of persons entitled to report and whether the report concerns misconduct that falls under the responsibility of the "Whistleblowing Officer (see "Information on the use of a whistleblowing system", section 3.1). If this is not the case, a corresponding response is sent to the whistleblower and the data received as part of the whistleblowing is deleted.

The Whistleblowing Officer also checks the validity of the report received, evaluates the evidence provided and, if necessary, asks the whistleblower questions. The Whistleblowing Officer then informs the Logwin group companies affected by the whistleblowing (usually the compliance officer of the respective Logwin group company).

Before any data is sent to Logwin, it will be **anonymised** by the Whistleblowing Officer **unless the whistleblower has expressly consented to the disclosure of their identity**. Any other superfluous personal data or information (i.e. data that is not relevant to the allegations in question) will also be removed by the Whistleblowing Officer before being sent to Logwin.

Please note that whistleblowing can always **be done anonymously**. You are neither obliged to disclose your identity to the Whistleblowing Officer.

Unless the whistleblower has expressly consented to the disclosure of their identity, the Whistleblowing Officer will act as an "intermediary" for any further communication between Logwin and the whistleblower (e.g. in case of queries from Logwin to the whistleblower).

b) Logwin shall follow up on the information received from the Whistleblowing Officer, including internal investigation, legal assessment, implementation of remedial measures and sanctioning. The Whistleblowing Officer may assist Logwin in this process.

3. What personal data is processed?

a) Whistleblower

In principle, all details and information of the whistleblower contained in the respective report, including any follow-up information, are processed. This may include the following data:

- The name of the whistleblower (unless the report has been made anonymously)
- All data and information disclosed in the report, in particular the description of the matter, including, for example, personal data about the whistleblower or about other persons.

If the Whistleblowing Officer is contacted by telephone or requests a face-to-face meeting, they may ask the whistleblower for consent to record the conversation or to make transcripts. Such consent will be recorded.

If the report to the Whistleblowing Officer is not made anonymously, the identity of the whistleblower will only be disclosed by the Logwin Whistleblowing Officer if the whistleblower has expressly consented to this.

b) Persons affected by the information (data subjects)

- Data contained in the whistleblower's information (e.g. names, positions, information about possible misconduct)
- Data necessary for the investigation of the information and for follow-up action, including, for example, data from the personnel file, information from colleagues or third parties, work-related documents and work-related communication.

Logwin will inform the respective data subjects in accordance with Art. 14 GDPR, insofar as the information would not make it impossible or seriously impair the effective investigation or the stopping or punishment of the allegations (Art. 14 (5) lit. b GDPR).

4. Legal basis

The legal basis for the data processing for the Whistleblowing Officer and Logwin is Art. 6 (1) lit. f GDPR, based on the following legitimate interests and purposes of Logwin:

- Detection and prosecution of violations pursuant to Art. 2 Whistleblowing Directive of Logwin, e.g. in the areas of money laundering and terrorist financing, product safety and compliance, environmental protection, consumer protection, protection of privacy and personal data, and security of networks and information systems;
- Implementation of legal obligations to which Logwin is subject, including, for example, ss. 130, 30 of the German Regulatory Offences Act (OWiG) and ss. 93, 111 of the German Stock Corporation Act (AktG);
- Preventing future misconduct;
- Compensation and defence of threatened economic or other damages or disadvantages for Logwin including legal defence, exercise and enforcement of Logwin's rights;
- Exoneration of persons wrongly suspected of misconduct;
- Examination of the relevance of the information for other Logwin group companies, including, if applicable, the disclosure of data to affected Logwin group companies.

All measures must take due account of the legitimate interests and fundamental rights and freedoms of the data subjects.

5. Data receiver

In addition to the data transfers between Whistleblowing Officers and Logwin described above, data transfers to the following receivers may be considered:

- Service providers who act as processors on behalf of the Whistleblowing Officer or Logwin and are obliged to maintain confidentiality accordingly (Art. 28 GDPR), e.g. technical service providers. The Whistleblowing Officer uses 1&1 IONOS as a hosting provider for the operation of their email accounts.
- Law firms and auditors who are subject to a legal or contractual duty of confidentiality;
- Courts and authorities;
- If there is a legitimate interest, other third parties, e.g. insurance companies, litigants or claimants;
- The persons directly or indirectly affected by the information (e.g. within the scope of internal investigations and clarification measures);
- Logwin Group companies if the matter also affects these Logwin Group companies.

6. Data deletion

If an information concerns misconduct that does not fall under the responsibility of the Whistleblowing Officer, the data received in the report will be deleted or anonymised after feedback to the whistleblower.

Otherwise, the data will usually be deleted or anonymised two months after completion of the investigation.

However, the legitimate interests of Logwin may also justify longer storage in individual cases. For example, data may also be retained for a longer period for the duration of an ongoing or anticipated legal dispute. The deletion periods of the individual cases depend on the specific legitimate interest of Logwin in retaining the data, taking into account in particular the importance of the retention for Logwin, the interests of the data subjects in the deletion or retention and the probability that the information is accurate.

7. Rights of data subjects

Beside the right to revoke any consent given to us, you are entitled to a right of information under Article 15 GDPR, a right to rectification under Article 16 GDPR, to deletion under Article 17 GDPR, to restriction of processing under Article 18 GDPR, a right to object to processing under Article 21 GDPR and a right to data portability under Article 20 GDPR if the respective legal prerequisites are met.

You have the right to object, on grounds relating to his or her particular situation, at any time to processing of your personal data which is based on Art. 6, (1) lit. f GDPR (Art. 21 (1) GDPR).

You can assert your rights both with and before the Whistleblowing Officer and before Logwin.

Moreover, you have the right to lodge a complaint with the relevant data protection supervisory authorities under Article 77 GDPR.

Status: 07/2026