



INFORMATION PURSUANT TO ARTICLE 13 OF GERMANY'S GENERAL DATA PROTECTION REGULATION (GDPR) CONCERNING THE PROCESSING OF PERSONAL DATA AS PART OF OUR WHISTLEBLOWER REPORTING SYSTEM

As at: May 2024

Hereinafter we inform you about the processing of personal data via the platform for reporting compliance breaches (whistleblower reporting system) provided on our website www.elbphilharmonie.com insofar as a report is not submitted anonymously.

Data Controllers

Elbphilharmonie und Laeiszhalle Betriebsgesellschaft mbH and HamburgMusik gGmbH, Platz der Deutschen Einheit 4, 20457 Hamburg are responsible for the processing of personal data and your related requests and queries.

The operational business is delivered through LegalTegrity GmbH, Platz der Einheit 2, 60323 Frankfurt, which is bound by instructions as the contractor as part of a data processing agreement with respect to the aforementioned companies.

Purpose of the Data Processing

The personal data, i.e. all the data with which a natural person can clearly be determined or who is at least identifiable via the information, are solely processed for the purpose of receiving notifications of compliance breaches in a secure and confidential way and following these up.

Categories of Data Processing as Part of the Whistleblower Reporting System

- Information about the whistleblower, unless this person would like to remain anonymous and the accused person(s), such as
 - first name and surname
 - role/title
 - contact details
 - if applicable, other personal data related to the employment contract
- Personal information which was identified in the reports from the whistleblower (see clause 4), including details of the allegations made and evidence supporting these
- Date and time of the calls (upon receipt of the notification via the telephone hotline)
- Any other information identified in the findings and in the additional procedures following the report, e.g. information concerning criminal conduct or data about unlawful or illegal conduct insofar as this was reported.

Legal Basis of the Data Processing

The collection of the personal data of the whistleblower from a non-anonymous notification is made on the basis of consent to processing via the transmission of data (implied consent) (Article 6 para. 1 clause 1 letter a GDPR).



The collection, processing and dissemination of the personal data of persons mentioned in the report serves to protect legitimate interests of the Elbphilharmonie und Laeiszhalle Betriebsgesellschaft mbH and

HamburgMusik gGmbH (Article 6 para. 1 clause 1 letter f GDPR). It is a legitimate interest of our company to uncover, process, remedy and where appropriate sanction significant breaches by employees effectively and with a high level of confidentiality and thereby prevent related damage and liability risks for the companies (Sections 30 and 130 of Germany's Act on Regulatory Offences [OWiG]). Germany's Whistleblower Protection Act also requires the establishment of a whistleblower reporting system to give employees and third parties in a suitable manner the opportunity to give notifications of legal violations in the companies safely.

The disclosure of personal data in the case of non-anonymous reporting to other recipients may be required due to a legal obligation (Article 6 para. 1 clause 1 letter c GDPR).

Recipient of the Data and Third Country Transmission (EU/EEA Countries)

Inspection of the stored data is solely possible by persons within the company specifically authorised for this or the lawyers appointed to accept and examine the reports received in the system. All persons authorised to inspect are expressly obliged to maintain confidentiality.

If the notification is received via the telephone hotline, the notification is recorded ensuring anonymity of the whistleblower in the whistleblower reporting system. The staff of the reporting office are obliged to maintain confidentiality (see below).

In some cases, there is the obligation to disclose the data to authorities (for example, those who have the legal or supervisory competence regarding the employer, law enforcement authorities and legal bodies) or external consultants (such as auditors, accountants, lawyers).

If personal data are processed by external service providers, this takes place in principle on the basis of data processing agreements in accordance with Article 28 GDPR. In these cases, we ensure that the processing of personal data is carried out in accordance with the provisions of GDPR and all persons authorised to process personal data have agreed to keep it confidential or are protected by adequate statutory rules on confidentiality.

Transmission of personal data in third countries (EU/EEA countries) does not take place.

Duration of Processing, Deletion of Data

The personal data are stored in the respective method as long as the information and final assessment requires it, the company has a legitimate interest or there is a legal requirement. Afterwards, these data are deleted in accordance with regulatory requirements. The duration of the retention is in particular in accordance with the severity of the suspicion and any breach of obligation reported. Retention may furthermore take place if this was stipulated by the European or national legislator to meet statutory requirements, such as record-keeping obligations. All personal data are then deleted.

Technical Information on the Use of the Whistleblower Reporting System

Communication between your computer and the whistleblower reporting system takes place via an encrypted connection (SSL). The IP address of your computer is not stored when you use the whistleblower reporting system. To maintain the connection between your computer and the whistleblower reporting system, a cookie is stored on your computer which only contains the session ID. This cookie is only valid until the end of your session and becomes invalid when you close your browser.

The whistleblower reporting system includes an option for anonymous communication via an encrypted connection. When you use it, your IP address and your current location are not stored at any time. After



submitting a notification, you assign a PIN and receive access data to the mailbox of the whistleblower reporting system in order to continue to be protected by us and, if desired, communicate anonymously.

We take appropriate technical measures to ensure data protection and confidentiality. The data you provide are stored on a particularly secure LegalTegrity database. All the data stored on the database are encrypted by LegalTegrity using the latest technology.

Rights of the Person Affected in Accordance with GDPR

When processing your personal data, the GDPR gives you specific rights. Please contact datenschutz@elbphilharmonie.de regarding this and let us know about your concerns.

- According to Article 7 GDPR, you shall have the right to **withdraw** your **consent** to the data processing at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- According to Article 14 GDPR, you shall have the right, if your data **are collected without your knowledge** (for instance because you are involved as the accused in proceedings to clarify the notification), **to be informed** of the storage, the type of data, the purpose of the processing and the identity of the data controller and, where appropriate, the whistleblower (unless the notification was submitted anonymously). If, however, the risk were considerable that such information would compromise the ability of the companies to effectively investigate the allegation or to collect the necessary evidence, this information may in accordance with Article 14 para. 5 clause 1 letter b GDPR be put on hold while this risk exists. The information must then be retrieved as soon as the reason for the delay has lapsed.
- According to Article 15 GDPR, you shall have the right to request **information** about the personal data relating to you, which are being processed by the companies.
- According to Article 16 GDPR, you shall have the right to request the immediate **rectification** or **completion** of inaccurate or incomplete data stored by us.
- According to Article 17 GDPR, you shall have the right to request the **deletion** of the personal data concerning you stored by us unless the processing is required to exercise the right to freedom of expression and information, to fulfil a legal obligation to which the companies are subject, to perform a task which is in the public interest or to establish, exercise or defend legal claims.
- According to Article 18 GDPR, you can request the **restriction** of the processing of your personal data if you contest the accuracy of these data or the processing of these data is unlawful.
- According to Article 20 GDPR, you shall have the right to receive the personal data concerning you in a structured, commonly used and machine-readable format and to **transmit** these data to another controller without hindrance or to have them transmitted by us.
- According to Article 21 GDPR, you shall have the right to **object** to the processing of your personal data insofar as there are grounds relating to your particular situation. Your data shall then no longer be processed unless the company can demonstrate compelling grounds for the processing, which override the interests, rights and freedoms of the person concerned or that the processing serves to establish, exercise or defend legal claims.
- You shall pursuant to Article 77 GDPR have the right to lodge a complaint with a supervisory authority if you are of the opinion that the processing of the data concerning you infringes data protection regulations. The right to lodge a complaint may in particular be asserted with a supervisory authority in the Member State of your habitual residence, your place of work or place of the alleged infringement.



Operational Data Protection Officer

Please contact our operational data protection officer for information or suggestions on the topic of data protection. She will be happy to help you:

Jennifer Jähn-Nguyen
datenschutz nord GmbH

www.dsn-group.de

office@datenschutz-nord.de

If you consult our data protection officer, please also state the responsible authority.