DATA PRIVACY NOTICE

Revision 2023 - due to HinSchG and new GBV

Data Privacy Notice

We take data protection and confidentiality very seriously and adhere to the provisions of the EU General Data Protection Regulation (EU-GDPR) as well as current national data protection regulations. Please read this data privacy information carefully before submitting a report.

Purpose and legal foundation of the whistleblowing system

The whistleblowing system (BKMS® Incident Reporting) serves the purpose or securely and confidentially receiving, processing and managing reports regarding violations of the compliance rules of GEMA, IT4IPM and ZSG. The processing of personal data in the BKMS® Incident Reporting is necessary to fulfil legal obligations and is based on the legitimate interest of our company in discovering to detect and prevent misconduct and thus avoid damage to GEMA, deecoob, IT4IPM and ZSG, their employees and customers. The legal basis for our processing of personal data is Article 6(1)c EU-GDPR in connection with § 10 HinSchG, if the notice is about a breach listed in § 2 HinSchG, and Article 6(1)c EU-GDPR in connection with § 8 LkSG regarding to notices about breaches of LkSG. In any other cases, the legal basis for our processing is Article 6(1)(f) EU-GDPR.

Responsible parties

The parties responsible for data privacy in the whistleblowing system are

1. GEMA - Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte and

its subsidiaries

2. deecoob GmbH (deecoob),
3. IT for Intellectual Property Management GmbH (IT4IPM) and
4. ZPÜ Service GmbH (ZSG)

as parties with mutually autonomous responsibility (hereafter also: “GEMA Group”).

Internal Reporting Channel for GEMA Group:

Internal Reporting
Channel Legal Departement/Compliance Rosenheimer Straße 11, 81667 Munich
compliance@gema.de
+49 (0) 89 48003 273

The whistleblowing system is operated by a specialised company, Business Keeper AG, Bayreuther Str. 35, 10789 Berlin in Germany, on behalf of the GEMA Group.

Personal data and information entered into the whistleblowing system are stored in a database operated by Business Keeper AG in a high-security data centre. Only selected employees of the Legal/ Compliance departments of GEMA can see the data. Business Keeper AG and other third parties do not have access to the data. This is ensured in the certified procedure through extensive technical and organisational measures.

All data are stored encrypted with multiple levels of password protection so that access is restricted to a very small selection of expressly authorised and specially trained persons in the Legal Departement / Compliance departments of GEMA.
The GEMA Group and its above-named subsidiaries have appointed a data protection officer. Inquiries regarding data protection can be sent to Dr. Sebastian Kraska at datenschutzbeauftragter@gema.de.

PDF: 07/02/24

Type of collected personal data

Use of the whistleblowing system takes place on a voluntary basis. If you submit a report via the whistleblowing system, we collect the following personal data and information:

- Your name, if you choose to reveal your identity,
- Whether you are employed at GEMA, deecoob, IT4IPM, ZSG or any other subsidiaries of GEMA Group, if you reveal this and
- The names and other personal data of persons that you name in your report, if applicable.

Confidential handling of reports

Incoming reports are received by a small selection of expressly authorised and specially trained employees of the GEMA Legal / Compliance departments and are always handled confidentially. The employees of the GEMA Legal / Compliance departments will evaluate the matter and perform any further investigation or follow-up actions required by the specific case.

While processing a report or conducting a special investigation, it may be necessary to share information of reports with additional persons, e.g. if the reports refer to incidents in subsidiaries. We will always ensure that the confidentiality and the applicable data privacy regulations are complied with when sharing information of reports.

All persons who receive access to the data are obligated to maintain confidentiality.

Information of the affected person

We are legally obligated to inform affected parties of any reports received about them as soon as the disclosure of this information doesn't jeopardise the investigation. In doing so, your identity as whistleblower is not revealed as far as is legally possible.

Rights of the data subjects
According to European data protection law, you and the persons named in the report have the right to inquiry, rectification, erasure, restriction of processing and the right to object to processing of personal data concerning them. If the right of objection is claimed, we will immediately examine to what extent the stored data is still necessary for the processing of a report. Data that is no longer required is deleted immediately. In addition, you have the right to lodge a complaint with a supervisory authority.

Retention period of personal data

Personal data is retained for as long as necessary to clarify the situation and perform an evaluation of the report or a legitimate interest of the company exists, or it is required by law. As a rule, personal data is deleted three years after the investigation has been completed in accordance with the statutory requirements.

Use of the whistleblowing portal

Communication between your computer and the whistleblowing system takes place over an encrypted connection (SSL). Your IP address will not be stored during your use of the whistleblowing system. In order to maintain the connection between your computer and the BKMS® Incident Reporting, a cookie is stored on your computer that merely contains the session ID (a so-called null cookie). This cookie is only valid until the end of your session and expires when you close your browser.
It is possible to set up a postbox within the whistleblowing system that is secured with an individually chosen pseudonym / user name and password. This allows you to send reports to the respectively responsible employee of the GEMA Legal Departement / Compliance department either by name or in an anonymous, safe way. This system only stores data inside the whistleblowing system, which makes it particularly secure. It is not a form of regular email communication.

Note on sending attachments

When submitting a report or an addition, you can simultaneously send attachments to the responsible employee of the GEMA Legal / Compliance department. If you wish to submit an anonymous report, please take note of the following security advice: Files can contain hidden personal data that could put your anonymity at risk. Remove such data before sending. If you are unable to remove this data or are uncertain about how to do so, copy the text of your attachment into your report text or send the printed document anonymously to the address listed in the footer, citing the reference number received at the end of the reporting process.

Version: October2023