HELMHOLTZ
MUNICH

Information pursuant to Art. 13 of the General Data Protection Regulation (GDPR) about the processing of personal data within the framework of the whistleblower system

In the following, we inform you about the processing of personal data by Helmholtz Zentrum München Deutsches Forschungszentrum für Umwelt und Gesundheit (GmbH) (hereinafter "HMGU") within the framework of the whistleblower system and about the associated data protection regulations, claims and rights.

The HMGU uses a web-based software, a cloud solution hosted in Germany, which assists in the detection of operational wrongdoing. By implementing such a system, criminal, illegal, morally reprehensible or unfair actions can be detected and prevented at an early stage. As a result, incalculable material and immaterial damages as well as reputational damage can be averted.

1. Purposes of data processing

The HMGU processes the personal data of the whistleblower(s), unless the whistleblowing is anonymous, as well as the personal data of the accused person(s), such as name and other communication and content data, exclusively for the purpose of receiving and following up on tips about criminal, illegal, morally reprehensible or unfair acts in a secure and confidential manner.

2. Categories of data processing

- Information about the whistleblower (unless the whistleblower wishes to remain anonymous) and the accused, such as
    - First and last name
    - Function/title
    - Contact details
    - Other personal information related to the employment relationship, if applicable
- Personal information identified in the reports of the team that investigates the facts of the case (see section 4), including details about the allegations made and evidence supporting those allegations
- The date and time of telephone calls (when the tip was received via the telephone hotline)
- Any other information identified in the investigation findings and in the follow-up process to the report, such as information about criminal conduct or data about unlawful or improper conduct, if reported

3. Legal basis of data processing

The collection of the whistleblower's personal data in the case of a non-anonymous whistleblowing is based on consent to the processing by the transmission of the data **(implied consent)** (Art. 6(1) point (a) GDPR).
The collection, processing and transfer of personal data of the persons named in the tip serves the **legitimate interests of the HMGU** (Art. 6(1) point (f) GDPR). It is a legitimate interest of the HMGU to detect, process, stop and sanction violations of the law and serious breaches of duty by employees center-wide, effectively and with a high degree of confidentiality, and to avert associated damage and liability risks for the HMGU (Sections 30, 130 of the Act on Regulatory Offences, OWiG). Directive (EU) 2019/1937 ("EU Whistleblower Directive") and the future “Whistleblower Protection Act” (currently in draft form) also require the establishment of a whistleblower system in order to provide employees and third parties with the opportunity to provide protected information about legal violations within the company in a suitable manner.
The disclosure of personal data to other recipients in the event of non-anonymous reporting may be necessary due to **a legal obligation** (Art. 6(1) point (c) GDPR).

4. Recipients of the data and third country transfer (Non-EU/EEA countries)

All personal data collected via the web-based software is only made accessible to those persons who have a legitimate need to process this data due to their function.

The HMGU has engaged an external lawyer for the initial processing of incoming tips. Lawyers are bound to secrecy by the professional law applicable to them.

If the tip is received via the telephone hotline, the tip is recorded in the whistleblower system while preserving the anonymity of the whistleblower. The hotline staff are bound to secrecy (see below).

At the HMGU only authorized employees from the following departments have access to the data (the team that investigates the facts of the case):

- Compliance Department
- Human Resources Department
- Legal Department
- Internal audit Department
- Good Scientific Practice (case-related)
- Complaints Department (case-related)

In some cases, the Legal & Compliance Department is required to disclose the data to authorities (such as those with legal or regulatory jurisdiction over the employer, law enforcement agencies and legal bodies) or external advisors (such as auditors, accountants, lawyers).

If the whistleblower has provided his/her name or other personal data (non-anonymous whistleblowing), the identity will not be disclosed – as far as legally possible – and it will also be ensured that no conclusions can be drawn about the identity of the whistleblower.

If personal data is processed by external service providers, this is generally done on the basis of contracts on processing on behalf of the controller in accordance with Art. 28 GDPR. In these cases, we ensure that the processing of personal data is carried out in accordance with the provisions of the GDPR and that all persons authorized to process personal data have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality. The whistleblower system is operated on our behalf by LegalTegrity GmbH, Platz der Einheit 2, 60327 Frankfurt/Main.

Personal data is not transferred to third countries (Non-EU/EEA countries).

5. Duration of processing, deletion of data

The personal data will be kept in each individual case as long as it is necessary for the investigation and the final assessment or there is a legitimate interest of the HMGU or a legal requirement. The duration of storage depends in particular on the severity of the suspicion and the reported possible breach of duty.

6. Technical instructions for using the whistleblower system

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

7. Rights of Data Subjects under the GDPR

You are entitled to the rights set out below in connection with the processing of your personal data:

- Under Art. 7 GDPR, you have the right to **withdraw your consent** to data processing at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- Under Art. 14 GDPR, if your data is collected **without your knowledge** (for example, because you are involved in the whistleblowing procedure as an accused person), you have the **right to be informed** about the storage, the nature of the data, the purpose of the processing and the identity of the controller and, if applicable, the whistleblower (unless the whistleblowing was done anonymously). However, if there would be a significant risk that such information would jeopardize the ability of the HMGU to effectively investigate

the allegation or gather the necessary evidence, this information may be postponed under Art. 14(5) point (b) GDPR for as long as this risk exists. The information must then be provided as soon as the reason for the postponement has ceased to exist.

- Under Art. 15 GDPR, you have the right to **access** any personal data relating to you that is processed by HMGU.
- Under Art. 16 GDPR, you have the right to the immediate **rectification** or **completion** of any inaccurate or incomplete data we hold about you.
- Under Art. 17 GDPR, you have the right to demand the **erasure** of all the personal data we hold about you, provided that processing is not required in order to exercise the right to freedom of expression and information; in order to comply with a legal obligation to which HMGU is subject; in order to complete a task that is in the public interest; or in order to establish, exercise or defend legal claims.
- Under Art. 18 GDPR, you may demand that **processing of your personal data be restricted**, if you contest the accuracy of the data, or the data is processed unlawfully.
- Under Art. 20 GDPR, you have the right to obtain the data we hold about you in a structured, commonly-used and machine-readable format, and to **transmit** that data to another controller without hindrance, or to arrange for us to **transmit** the data.
- ***Under Art. 21 GDPR you have the right to object, on grounds relating to your particular situation, to processing of your personal data. The HMGU will then no longer process your personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.***
- Under Art. 77 GDPR, Sec. 17 BDSG, you have the right to lodge a **complaint** against HMGU with the relevant supervisory authority, specifically:

  Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
  Husarenstr. 30, 53117 Bonn
  Tel.: +49 (0)228-997799-0
  E-Mail: poststelle@bfdi.bund.de

8. Controller's contact details

The Controller in relation to the processing of the personal data described above, and to any requests or queries associated with it, is:

Helmholtz Zentrum München
Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH)
Ingolstädter Landstraße 1
D-85764 Neuherberg

If you have any questions regarding data protection, please contact our Data Protection Officer:

Werner Bergheim
Helmholtz Zentrum München
Deutsches Forschungszentrum für Gesundheit und Umwelt (GmbH)
Ingolstädter Landstraße 1
D-85764 Neuherberg
E-Mail: datenschutz@helmholtz-muenchen.de