Information pursuant to Article 13 of the General Data Protection Regulation (GDPR) on the processing of personal data in the context of the whistleblower system

In the following, we inform you about the processing of personal data by CDS Hackner GmbH (hereinafter " CDS Hackner") in the context of the whistleblower system as well as about the associated data protection regulations, claims and rights.

CDS Hackner GmbH (Rossfelder Straße 52/5, 74564 Crailsheim) uses 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. In this way, incalculable material and immaterial damage as well as reputational damage can be averted.

1. **Purpose of the data processing**

   CDS Hackner 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 investigating tips about criminal, illegal, morally reprehensible or unfair acts in a secure and confidential manner.

2. **Categories of data processing in the context of the whistleblowing system**
   - Information about the whistleblower (unless he/she wishes to remain anonymous) and the accused, such as
     - First and last name
     - Function/Title
     - Contact details
     - If applicable, other personal data related to the employment relationship
   - Personal information identified in the intelligence team's reports (see paragraph 4), including details of the allegations made and evidence supporting those allegations
   - Date and time of the calls (when the tip is received via the telephone hotline)
   - Any other information identified in the investigation findings and in the follow-up procedure following the report, e.g. information on criminal conduct or data on unlawful or improper conduct, where this has been reported

3. **Legal basis of the 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 through the transmission of the data (implied consent) (Art. 6 para. 1 sentence 1 lit. a DSGVO).

The collection, processing and disclosure of personal data of the persons named in the notification serves the **legitimate interests** (Art. 6 para. 1 p. 1 lit. f DSGVO). It is a legitimate interest of the companies to uncover, process, stop and sanction violations of the law and serious breaches of duty by employees centre-wide, effectively and with a high degree of confidentiality and to avert associated damage and liability risks for the companies (Sections 30, 130 OWiG). Directive (EU) 2019/1937 ("EU Whistleblower Directive") and the future Whistleblower Protection Act also require the establishment of a whistleblower system in order to give employees and third parties the opportunity to provide protected information on legal violations in the company in a suitable manner.

The disclosure of personal data to other recipients in the case of non-anonymous reporting may **be necessary** due to a **legal obligation** (Art. 6 para. 1 p. 1 lit. c DSGVO).

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

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

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

In some cases, the company is required to share the data with authorities (such as those having 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 whistleblower), 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 will generally be done on the basis of order processing contracts in accordance with Article 28 of the 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 authorised to process personal data have committed themselves to confidentiality or are subject to an appropriate legal duty of confidentiality. The whistleblower system is operated by LegalTegrity GmbH, Platz der Einheit 2, 60327 Frankfurt am Main.

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

5. **Duration of processing, deletion of data**

   The personal data will be kept in the respective proceedings for as long as the clarification and final assessment requires, a legitimate interest of the company or a legal requirement exists. Afterwards, this data is deleted in accordance with the legal requirements. The duration of storage depends in particular on the severity of the suspicion and the reported possible breach of duty.

6. **Technical notes on the use of the whistleblowing 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 whistleblowing 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 your browser.

7. **Use of Friendly Captcha**

   Our website uses the „Friendly Captcha“ service (www.friendlycaptcha.com).

   This service is offered by Friendly Captcha GmbH, Am Anger 3-5, 82237 Wörthsee, Germany. Friendly Captcha is a new, privacy-friendly protection solution to make it more difficult for automated programs and scripts (so-called "bots") to use our whistleblower application.

   For this purpose, we have integrated a program code from Friendly Captcha into our application before a message is sent so that the visitor's terminal device can establish a connection to the Friendly Captcha servers in order to receive a calculation task from Friendly Captcha. The visitor's terminal solves the calculation task, which requires certain system resources, and sends the calculation result to our web server. The server contacts the Friendly Captcha server via an interface and receives a response stating whether the end device solved the calculation correctly. Depending on the result, we can apply security rules to requests via our website and, for example, process or reject them.

   The data is used exclusively to protect against spam and bots as described above. Friendly Captcha does not set or read any cookies on the visitor's terminal device. IP addresses are only stored in hashed (one-way encrypted) form and do not allow us and Friendly Captcha to draw any conclusions about an individual person. If personal data is stored, this data is deleted within 30 days.

   The legal basis for the processing is our legitimate interests in protecting our website against abusive access by bots, i.e. spam protection and protection against attacks (e.g. mass requests), Art. 6 para. 1 lit. f DSGVO.

   For more information on data protection when using Friendly Captcha, please visit https://friendlycaptcha.com/legal/privacy-end-users/.

8. Data subject rights under the GDPR

You have the following rights in relation to the processing of personal data relating to you:

- According to Art. 7 DSGVO, you have the right to **revoke** your **consent to** data processing at any time. The revocation of consent does not affect the lawfulness of the processing carried out on the basis of the consent until the revocation.
- According to 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 jeopardise the companies' ability to effectively investigate the allegation or gather the necessary evidence, this information can be postponed according to Art. 14 (5) p. 1 lit. b DSGVO 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.
- In accordance with Art. 15 of the GDPR, you have the right to request **information about the personal** data concerning you that is processed by the companies.
- In accordance with Art. 16 DSGVO, you have the right to request the immediate **correction** or **completion of** incorrect or incomplete data stored by us.
- Pursuant to Art. 17 DSGVO, you have the right to request the **erasure of** personal data concerning you that is stored by us, unless the processing is necessary for the exercise of the right to freedom of expression and information, for compliance with a legal obligation to which the company is subject, for the performance of a task carried out in the public interest, or for the establishment, exercise or defence of legal claims.
- Pursuant to Art. 18 DSGVO, you may request the **restriction of the** processing of your personal data if you dispute the accuracy of such data or if the processing of such data is unlawful.
- In accordance with Art. 20 DSGVO, you have the right to receive the personal data concerning you in a structured, common and machine-readable format, and to **transmit** this data to another controller without hindrance or to have it transmitted by us.
- Pursuant to Art. 21 DSGVO, you have the right to **object to the** processing of your personal data, where there are grounds for doing so based on your particular situation. Your data will then no longer be processed unless the company can demonstrate compelling grounds for the processing which override the interests, rights and freedoms of the data subject, or for the assertion, exercise or defence of legal claims.

- According to Art. 77 DSGVO in conjunction with. § 17 BDSG, you have the right to lodge a **complaint** against companies with the competent supervisory authority. This is:

The baden-württembergian Commissioner for Data Protection and Freedom of Information

PO Box 10 29 32

70025 Stuttgart

Phone: +49 711 615 541-0

9. Verantwortlicher im Sinne des Datenschutzrechts

Responsible for the processing of the above personal data and your related applications and requests is the:

CDS Hackner GmbH, Rossfelder Straße 52/5, 74564 Crailsheim
Managing Director Michael Hackner

Tel: +49 7951 391-0