Privacy policy for the whistleblower system

HMF Smart Solutions GmbH (hereinafter referred to as "**HMF**", "**we**", "**us**") demands and promotes transparent business activities. We are fully committed to compliance. Reliability, integrity and compliance form the foundation of our activities.

The Whistleblower Protection Act (HinSchG) came into force on 2 July 2023. This law regulates the protection in particular of natural persons who have obtained information about violations in connection with their professional activities or in advance of a professional activity and disclose this information. By reporting, you contribute to the prevention, detection and elimination of errors in our company.

We would therefore like to encourage you as a reporting person (employee or external party) to contact our internal reporting centre (whistleblower system) with suspicious facts, providing as much specific information as possible.

Below we inform you in accordance with Art. 13 and 14 of the EU General Data Protection Regulation (**GDPR**) about the processing of your personal data (hereinafter referred to as "**data**") as part of our whistleblower system. We will only process the data within the framework of the whistleblower system in accordance with the applicable data protection regulations. These requirements result in particular from the GDPR and the German Federal Data Protection Act (**BDSG**). This data protection information supplements our general data protection information for employees.

For reasons of better readability, the simultaneous use of the language forms male, female and diverse (m/f/d) is omitted. All personal designations apply equally to all genders.

Who is responsible for the processing of your data

Responsible for the processing of your data is

HMF Smart Solutions GmbH
Fritz-Hahne-Straße 7
D-31848 Bad Münder

Telephone: + 49 (0) 5042 998 0
E-mail: info@hmf-germany.com

You can reach our **data protection officer** either at

datenschutz@hmf-germany.com

or

at the above postal address with the addition "Data Protection Officer".

How to report?

Internal reporting centre
Information can be submitted via an online reporting form. These are dealt with and processed as part of a regulated procedure.

External reporting centre of the federal government
In addition to reporting information about an offence to the internal reporting office, you can also report it to an external reporting office. The federal government's external reporting centre is located

at the Federal Office of Justice (BfJ). The reporting channels and further information on the BfJ's external reporting centre are published on the BfJ website.

Section 7 para. 1 sentence 1 HinSchG provides for a right of choice. However, according to Section 7 para. 1 sentence 2 HinSchG, whistleblowers should prefer to report to an internal reporting centre in cases where effective internal action can be taken against the violation and they do not have to fear reprisals. We therefore ask you to first contact our confidential internal reporting centre with any suspicious circumstances.

Who can report violations and which violations can be reported?

Information can be reported by employees, business partners, suppliers and other third parties. This confidential process is made available to reporters to report suspected violations of laws or regulations, the Code of Conduct or other HMF internal policies. Please note that use of the online reporting form is entirely voluntary. HMF employees are encouraged to report possible violations directly to their supervisor or the HR department. If you feel unable or uncomfortable to do so, you can of course use the online reporting form to submit your reports.

The online reporting form is exclusively for receiving and processing reports of actual or suspected violations of laws, guidelines or HMF's Code of Conduct. Possible violations are e.g:

- Corruption and bribery, fraud, money laundering and embezzlement;
- Violations of human rights;
- Discrimination or harassment;
- Violations of antitrust and competition law;
- Environmental, health and safety issues;
- Conflicts of interest;
- breaches of confidentiality, market abuse and insider trading regulations;
- Violations of the Product Safety Act and the Product Liability Act;
- Industrial espionage;
- Unauthorised disclosure of information;
- Falsification of annual reports and business documents;
- data manipulation;
- Violations of data protection and IT security regulations; and
- Retaliation against individuals who have spoken out in good faith.

The list is not exhaustive. If your concern relates to an offence that is not listed, please contact your line manager or the HR department in your capacity as an employee.

Please be aware that the information you provide about yourself, your colleagues or other aspects of HMF business activities may lead to decisions that affect other people. Therefore, we ask that you only provide information that you believe to be true. We will not retaliate against you for reporting a potential violation in good faith, even if it later turns out to be factually incorrect. Please note, however, that knowingly providing false or misleading information will not be tolerated. The information you provide will be kept confidential, except in cases where this is not possible due to legal requirements or to conduct an investigation. We encourage you to disclose your identity so that we can better process your request and follow up on any queries.

What data is processed?

In principle, the service can be used anonymously, i.e. without providing your data. However, you can voluntarily disclose your data, including information about your identity, your first and last name,

your telephone number or your e-mail address. If you provide this data voluntarily, it will be processed by us. This privacy policy applies in addition to our existing general privacy policy, which provides you with specific information on how we process your data when you visit our website.

Special categories of personal data, such as information on racial and/or ethnic origin, religious and/or ideological beliefs, trade union membership or sexual orientation, are not requested or processed by us. However, thanks to the free text field in the online form, you can voluntarily provide such special categories of personal data.

The notification you submit may also contain data from third parties to whom you refer in your notification. These data subjects have the opportunity to comment on the information. In this case, we will inform the persons concerned about the report or the information provided. Your confidentiality is also guaranteed in this case, as the person concerned will - as far as legally possible - not receive any information about your identity and your information will be used in such a way that your anonymity is not jeopardised.

Please note that it is often required by law that the persons who are the subject of a report or tip-off must be notified and heard. During the investigation, these persons have the opportunity to present their views on the report. The data subject may have a right to information under applicable laws that could compel us to disclose their identity. Government agencies may also have similar rights of access or seizure that result in the disclosure of your identity. This may be the case in particular if the person concerned claims that the information provided against them is intentionally or grossly negligently untrue and then decides to press charges.

What happens after the report?

The initial assessment of the incident is carried out by the responsible investigator (HR department), who will confirm receipt of the report to you in writing within 7 days. If, after the initial assessment, the investigator concludes that there is no evidence of relevant misconduct, he will discontinue the procedure and inform you in writing as soon as possible of his decision and the reasons for it.

If, following an initial assessment, the investigator concludes that there is evidence of relevant misconduct, appropriate action will be taken, which may include appointing one or more individuals (either within or outside HMF) to investigate the disclosure. The investigator(s) will provide you with feedback no later than 3 months from the date of acknowledgement of receipt of the report. The feedback will include information on the progress of the investigation and its expected timeframe.

For what purposes is your data processed? What is the legal basis for processing your data?

We process your data within the framework of the applicable laws, in particular for the following specific compliance and information purposes:

- Checking the plausibility of reports
- Clarification of misconduct
- Implementation of legal obligations
- Prevention of future misconduct
- Exercise of rights
- Relief of employees
- Implementation of duties to co-operate.

In addition, the purposes listed in the general data protection information for employees may also be considered as possible purposes of data processing.

The collection, processing and disclosure of your data in the context of the reports is carried out in accordance with the applicable data protection laws, including the GDPR and the Federal Data Protection Act (BDSG).

Implementation of legal obligations: If the notification falls within the scope of the HinSchG, the legal basis for the processing of your data in connection with this notification is Section 10 HinSchG in conjunction with Art. 6 para. 1 lit. c GDPR. Art. 6 para. 1 lit. c) GDPR.

Safeguarding legitimate interests: In all other cases, the processing of your data in relation to a (potential) infringement is based on our legitimate interest in investigating infringements, receiving reports of infringements and processing them in accordance with the standards and values we have established (Art. 6 para. 1 lit. f) GDPR). Our legitimate interests may include in individual cases

- Legal defence
- Improvement of the compliance structure
- Support of data subjects
- Implementation of foreign legal provisions.

Investigation of criminal offences: The processing of data relating to criminal offences is carried out in accordance with Art. 10 GDPR (and, if applicable, Section 9 (2) HinSchG). If reconnaissance measures serve to uncover possible criminal offences in the context of employment relationships, these may be justified in accordance with Section 26 (1) sentence 2 BDSG. However, we will only base such data processing on Section 26 (1) sentence 2 BDSG in conjunction with Art. 6 (1) lit. Art. 6 para. 1 lit. b) GDPR if documented factual indications justify the suspicion of a criminal offence in the employment relationship and the interests of the data subject do not prevail.

Implementation of the employment relationship (Section 26 (1) sentence 1 BDSG in conjunction with Art. 6 (1) (b) GDPR): Data processing in the context of reconnaissance measures may be necessary, among other things, for the implementation and termination of the employment relationship with employees. This applies, for example, to reconnaissance measures to uncover breaches of duty under employment contracts that do not constitute a criminal offence. Investigative measures may also be necessary for the settlement of employment relationships. This may be the case, for example, if we impose labour law sanctions against a person concerned on the basis of the findings obtained in the course of an investigative measure.

Company agreements (Art. 88 para. 1 GDPR, Section 26 para. 4 BDSG): We may also process your data on the basis of a valid company agreement that regulates the introduction and operation of the whistleblowing system.

Consent: In addition, data may be processed on the basis of Art. 6 para. 1 lit. a) GDPR if the reporting person has given consent.

Processing of special categories of personal data: If, in exceptional cases, special categories of personal data are processed (sensitive data), the legal basis for the processing is Art. 9 GDPR, Section 10 HinSchG and Section 22 BDSG.

We do not intend to use your data for purposes other than those mentioned above.

Who are the recipients of your data?

Initially, only authorised persons gain knowledge of the data transmitted by the ombudsman's office in pseudonymised form. Appropriate authorisation systems and appropriate technical and organisational measures ensure that only the relevant persons have access to this data. The persons entrusted with processing the incidents are expressly obliged to maintain confidentiality.

In order to fulfil the aforementioned purpose, it may also be necessary for us to transfer your data to external bodies such as law firms, criminal or competition authorities, authorities within or outside the EU/EEA.

In certain situations, your data may be transferred to a country outside the EU/EEA or to a country with an adequate level of data protection. In such a case, HMF will ensure that the standard contractual clauses of the EU Commission are concluded with the recipient of the data and that all relevant additional guarantees are ensured.

How long will your data be stored?

Your data will be stored in accordance with the applicable data protection laws and deleted 3 years after completion of the procedure (§ 11 para. 5 HinSchG). In certain cases and for certain documents, a longer period may be appropriate. Data may also be stored if this is required by European or national legislation to fulfil legal obligations, such as retention obligations. All data will then be deleted, blocked or anonymised.

What data protection rights do you have?

You have extensive rights with regard to the processing of your data.

Right to information: You have the right to information about the data stored by us, in particular the purpose for which the data is processed and how long the data is stored (Art. 15 GDPR). This right is limited by the exceptions of Section 34 BDSG, according to which the right to information does not apply in particular if the data is only stored due to statutory retention regulations or for data backup and data protection control, the provision of information would require a disproportionate effort and misuse of the data processing is prevented by suitable technical and organisational measures.

Right to rectification of inaccurate data: You have the right to obtain from us without undue delay the rectification of inaccurate personal data concerning you (Art. 16 GDPR).

Right to erasure: You have the right to obtain from us the erasure (Art. 17 GDPR) of data concerning you. These conditions apply in particular if a) the respective processing purpose has been achieved or otherwise ceases to apply, b) we have processed your data unlawfully, c) you have withdrawn your consent without the data processing being able to continue on another legal basis, d) you successfully object to the data processing or e) in cases where there is an obligation to erase based on the law of the EU or an EU member state to which we are subject. This right is subject to the restrictions set out in Section 35 BDSG, according to which the right to erasure may not apply in particular if, in the case of non-automated data processing, a disproportionately high effort is required for erasure and your interest in erasure is considered to be low.

Right to restriction of processing: You have the right to request that the processing of your data be restricted (Art. 18 GDPR). This right exists in particular if a) the accuracy of the data is disputed, b) you request restricted processing instead of deletion under the conditions of a justified request for deletion, c) the data is no longer required for the purposes pursued by us, but you need the data for the assertion, exercise or defence of legal claims or d) the success of an objection is still disputed.

Right to data portability: You have the right to receive the data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format (Art. 20 GDPR), provided that it has not already been erased.

Right to object: You have the right to object, on grounds relating to your particular situation, at any time to processing of data concerning you (Art. 21 GDPR). We will stop processing your data unless

we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or if the processing serves the establishment, exercise or defence of legal claims.

In accordance with Art. 7 para. 3 GDPR, you have the right to revoke your consent to us at any time. The revocation does not affect the legality of the processing carried out on the basis of the previous consent. The only consequence of the revocation is that we may no longer continue the data processing based on this consent in the future. Please note, however, that we may not be able to provide certain services or additional services if we are unable to process the data required for this purpose.

Right in connection with automated decision-making: You have the right (Art. 22 GDPR) not to be subject to automated decision-making, including profiling, which produces legal effects concerning you or similarly significantly affects you. We generally do not use automated decision-making or profiling in employment matters. However, if you have been subject to an automated decision and do not agree with the outcome, you can contact us in the ways set out below and ask us to review the decision

Right to lodge a complaint with the supervisory authority: You have the option of contacting the above-mentioned data protection officer or a data protection supervisory authority if you believe that the processing of data concerning you is in breach of the GDPR.