Privacy policy

on the processing of personal data in the whistleblower system

The purpose of the whistleblower system is to give all persons regardless of their gender or personal orientation and associated with the Hipp Group, for example employees, suppliers, customers, consumers, interns, trainees, volunteers, temporary workers, job applicants, self-employed persons, members of an administrative or management body, contractors and subcontractors (hereinafter also referred to as "whistleblowers"), the opportunity to report relevant and serious misconduct that has occurred or is alleged to have occurred within the organization.

This is an important tool for minimising risk and maintaining trust in our activities. It enables the persons appointed to audit (hereinafter also referred to as "we" and "auditors"), namely the Group Compliance Manager and the representatives appointed by him, as well as any ombudsmen appointed by Hipp, to take action at an early stage.

The whistleblower system (the "System") is provided by a processor, an external party commissioned by Hipp GmbH & Co. Vertrieb KG under the leadership of the Group Compliance Manager to process personal data on its behalf. The system enables whistleblowers to submit anonymous reports in a technically secure manner. Anonymity is hereby expressly guaranteed by the Group Compliance Manager.

This Privacy Policy describes how we collect and use your personal data in accordance with the legal requirements, namely the General Data Protection Regulation (EU) 2016/679 applicable in the European Union, hereinafter referred to as "**GDPR**", and process it to fulfil our legal obligations under Directive (EU) 2019/1937 of the European Parliament and of the Council on the protection of persons who report breaches of Union law (the "**Directive"**) and the relevant national implementing laws. This Privacy Policy also describes your rights and how you can exercise them.

If you have any questions or comments about data protection and our processing of your personal data as described here, you can contact the **Group Compliance Manager** at any time by e-mail (Alexander.Maier@hipp.de) or in any other way.

1 PERSONAL DATA THAT WE PROCESS, PURPOSE OF PROCESSING AND LEGAL BASIS

Personal data that we can process	• Surname, first name, contact details, function(s) of the reporter (unless anonymity is chosen) • Surname, first name, contact details, function(s) of the accused/affected/involved/witnesses or persons involved in any other way

	• a description of the event, time and place and any other information that the reporter considers relevant (depending on the type of report, the processed data may contain personal data and these may also belong to special categories of personal data); • Information on how notifications are created, processed and transmitted (including notification code and status) • Other information provided by the applicant that contains personal data; • Information about the persons who process the reports received via the system, e.g. name, job title, e-mail address, user ID.
Purpose of the processing	• The reporter is enabled to present relevant and serious events in order to enable the auditors to recognise and investigate irregularities and, if necessary, to prepare and initiate legal action or involve third parties, in particular the authorities.
Legal basis for the processing	• For the fulfilment of a contract (Article 6(1)(b) of the GDPR); • To fulfil a legal obligation (Article 6(1)(c) of the GDPR); • For the purposes of legitimate interests (Article 6(1)(f) of the GDPR); • In cases where notifications contain information about special categories of personal data, the processing of this information may be necessary for the preparation, exercise or defence of a legal claim under Article 9(2)(f) of the GDPR.

2 HOW WE COLLECT YOUR PERSONAL DATA

The information originates from the person making the report and may be supplemented by information that the investigator believes comes from a secure source and may be useful for the investigation. This data is stored in an area of the system protected against unauthorised access, supplemented and corrected if necessary.

3 PRINCIPLE OF CONFIDENTIALITY OF IDENTITY AND INVOLVEMENT OF THIRD PARTIES

The whistleblower protection laws oblige operators and auditors to maintain whistleblower systems in such a way that the confidentiality of the identity is ensured:

- of the person(s) providing the information,
- the person(s) affected by the notification,
- and any other persons named in the notification.

This confidentiality obligation represents a central protective measure.

Permitted exceptions to data transfer

The duty of confidentiality ends where the law exceptionally provides for disclosure/disclosure!

a) Consent of the data subject: Disclosure is permitted if the data subject has expressly consented.

b) Necessity for processing the report: If the disclosure is necessary to clarify the reported facts or to take measures (e.g. internal investigations, labour law steps), it may be made - but only to the competent bodies and in compliance with the principle of proportionality.

c) Legal obligations or official orders: Disclosure may also be necessary if:

- there is a legal obligation to disclose (e.g. to law enforcement authorities),

- a court or official order has been issued,

- or disclosure is necessary for the defence against legal claims.

Notwithstanding the above provisions, the data may be forwarded to:

- **Lawyers. Experts.** They are bound by professional or contractual confidentiality. In addition to our auditors, lawyers or other experts bound to confidentiality may be involved by the auditor in the processing and follow-up of whistleblower reports if this appears expedient to clarify the facts of the case, to clarify legal issues or for the auditor's assessment.

  Authorities. In accordance with legal requirements, information may also be forwarded to authorities, namely police stations, if there is a suspicion of a criminal offence or misdemeanour.

  Processor. Your personal data is passed on to our processor so that it can be made available in the whistleblowing system. In this context, our processor also uses service providers to provide its services . Our processor is not authorised by us to use or disclose your personal data unless this is necessary for the provision of the service or to comply with legal requirements. We only authorise our suppliers or subcontractors to use your personal data for the purposes of providing the service.

- **Mergers, acquisitions or other business transfers.** In the unlikely event of a merger, sale of company assets, financing or takeover of all or part of a company by

another company during the use of the whistleblower system, this may also result in a disclosure or transfer, subject to strict confidentiality.

Finally, the identity of the declarant may be disclosed if this is necessary for the competent authority to establish the validity of the declaration and to prevent a possibly unjustified, wilful, for the investigating authorities or the public prosecutor to fulfil their tasks or to prepare, assert or defend a legal claim.

4 WHERE WE PROCESS YOUR PERSONAL DATA

We will always endeavour to process and store your data within the EU/EEA. However, in certain situations, your data may be transferred to relevant recipients on a need-to-know basis as described above. For example, we may be required by law to disclose your personal data to authorities both in the country in which you and we are based and abroad. This could mean that your personal data is transferred to third countries outside the EU/EEA area.

Please note that data protection laws in countries outside the EU/EEA may in some cases offer less protection than the data protection laws in your country. However, we always choose our service providers carefully and take all necessary measures to ensure that your personal data is processed with appropriate safeguards (e.g. standard contractual clauses in accordance with Article 46 (2) (c) GDPR or on the basis of an adequacy decision of the EU Commission in accordance with the GDPR.

5 HOW LONG WE KEEP YOUR PERSONAL DATA FOR

The data will be stored for the maximum statutory retention period under national law for 10 years after the whistleblower case has ended. After this period has expired, your personal data will be deleted or anonymised unless we are legally obliged to retain it.

The log of the reports submitted, the contains the names of the persons involved in the investigations, is kept for 10 years for the purposes of compliance checks, after which it is checked whether further storage is necessary.

6 YOUR RIGHTS

- **Right to information and access to your data.** You have the right to request information about how we process your data and to receive a copy of the personal data processed by us. The first copy can be requested free of charge. However, if you repeatedly and unreasonably request copies, we may charge you an administrative fee
- **Right to rectification.** You have the right to correct inaccurate or incomplete information.
- **Right to erasure ("right to be forgotten").** You have the right to request that we erase personal data about you, e.g. if the data is no longer necessary in relation to the purposes for which it was collected or otherwise processed or if there is no legal basis for processing the data.

- **Right to restriction.** You have the right to request that the processing of your personal data be restricted until incorrect or incomplete information about you has been corrected or an objection from you has been processed.
- **Right to object.** You have the right to object to processing on the basis of a legitimate interest. This means that we may no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests.
- **Right to withdraw your consent.** You can withdraw your consent at any time. Please note, however, that this has no effect on any processing that has already taken place.
- **Right to lodge a complaint.** You have the right to lodge a complaint with the supervisory authority of the country in which you live or work if you believe that we have failed to fulfil our obligations in relation to your personal data. In the European Union and the European Economic Area, the supervisory authority responsible, also for coordination with local authorities, is the Bavarian State Office for Data Protection Supervision, P.O. Box 606, D-91511 Ansbach, poststelle@lda.bayern.de.

Please note that our legal rights or obligations may prevent us from disclosing or transferring all or part of your data or deleting your data immediately.

Please contact us using the following contact details to assert your rights.

Controller

Hipp GmbH & Co. Vertrieb KG, Georg-Hipp-Str. 7, 85276 Pfaffenhofen/Ilm, for the attention of A. Maier by e-mail: datenschutz-team@hipp.de

7 EXCEPTIONS TO THE RIGHTS OF THE DATA SUBJECT

The right to information does not apply to data that could reveal the identity of the whistleblower.

Please also note that according to Article 14(5)(b) of the GDPR, the right of access is restricted if the information would be likely to render impossible or seriously impair the achievement of the objectives of that processing (investigation of a whistleblower case).

8 SAFETY MEASURES

The system is encrypted and password-protected to ensure the anonymity of the whistleblower. Messages received via the system are only received and processed by authorised personnel. No IP addresses are registered in the system and the system does not use cookies. All data transmission and storage of personal data is encrypted to prevent it from being falsified or coming to the attention of unauthorised persons.

9 CHANGES TO THIS PRIVACY POLICY

We may change and update this Privacy Policy. We will inform you of any significant changes to this privacy policy or our processing of your personal data.

23.05.2025AM