Customer / Supplier Data Privacy Policy

(As of May, 2025)

1. Purpose of this privacy policy

We take data protection seriously and hereby inform you, how we process your data and which claims and rights you are entitled to under the data protection regulations.

Responsible for data processing and contact details:

Responsible for the processing of the data within the meaning of the General Data Protection Regulation is:

Dunhills (Pontefract) PLC

26 Front Street

Pontefract, West Yorkshire

WF8 1NJ

E-Mail: dataprivacy@haribo.com

Telephone: +44 (0) 1977 600266

2. Purpose and legal basis on which we process your data:

We process personal data in accordance with the provisions of the General Data Protection Regulation (GDPR) which includes UK GDPR and EU GDPR, the Data Protection Act 2018 (DPA) and other applicable data protection regulations. Please see further details below:

2.1 Purpose for the performance of a contract or pre-contractual measures:

We process personal data (name, e-mail address, job title, title, telephone numbers, billing address, bank details, address) that you provide to us or give us access to as is necessary in order to take the requisite steps to enter into, and for the performance of, our contract with you (GDPR Article 6(b)). For example, as provided in the context of the preparation for or conclusion of the contract, for the provision of products or services or as otherwise takes place for the establishment, implementation and possible termination of our contract(s) with you and the execution of relevant orders. We may process data that we receive in the course of a complaint in order to examine the incident and process it. We also use our customers' data to recover our claims.

2.2 Purposes in the context of a legitimate interest of us or third parties:

In addition to the actual fulfillment of the (pre-)contract, we process your data if necessary, in accordance with our legitimate interests or interests of third parties, unless your interests or fundamental rights and freedoms conflict with this (GDPR Article 6(f)). Eligible interests may include: our economic interests, our legal interests, our interest in compliance and ensuring compliance or even IT security.

Authorised interests are for example:

- undertaking credit checks and receiving information from credit reference agencies (please see section 2.4 below);
- quality control and review and communication procedures;
- review by affiliated companies (such as the parent company) or the respective supervisory bodies or supervisory bodies (e.g. auditors) as well as risk management in the HARIBO Group of companies;
- measures for business control, further development of services and products;
- collection of claims by debt collection agencies;
- asserting legal claims and defense in legal disputes;
- ensuring IT systems / IT security;
- video surveillance to safeguard the premises and for the prevention of criminal acts;
- measures for building and plant safety (for example access control);
- prevention and investigation of criminal offences;
- verifiability of orders, inquiries, etc., and other agreements as well as for quality control and training purposes by recording telephone calls;

2.3 Purposes for the fulfillment of legal requirements:

As a business, we are subject to a variety of legal obligations. These are primarily legal requirements (such as, but not limited to, commercial and tax laws), but also, if necessary, other regulatory requirements. As a result we may process data to the extent necessary for us to comply with our legal obligations (GDPR Article 6(1)(c)). Processing may include identity and age checks, prevention of fraud and money laundering, prevention, combating and resolution of terrorist financing and offending criminal acts, compliance with fiscal control and reporting obligations and the archiving of data for privacy and data security purposes and audit by tax and other authorities.

In addition, to the extent necessary in accordance with our legitimate interest (see section 2.2 above), we may need to disclose personal data in the context of administrative / judicial action. The legitimate interest in this case would be for the purposes of gathering evidence, prosecuting or enforcing civil claims.

2.4 Purpose of the credit check and data transmission to credit bureaus:

We use the data provided by you (name, address, date of birth and possibly gender) for the application, execution and termination of the business relationship. We process your data for inquiries and credit reports based on mathematical-statistical procedures at credit reference agencies for your creditworthiness before the conclusion of a contractual relationship check. We may also transfer data on non-contractual behavior or fraudulent behavior during the contractual relationship to a credit reference agency. The exchange of data with a credit reference agency also serves the purpose of identity verification. We can use the compliance rates provided by the credit reference agency to determine if a person is stored in their database at the address provided by the customer.

Insofar as we obtain a query from a credit reference agency, the legal basis is as is necessary for the performance of a contract (Article 6(1)(b)). Insofar as we pass on information about non-contractual behavior to a credit reference agency, the legal basis is as is necessary in accordance with the legitimate interests of HARIBO or of third parties and does not outweigh your interests or fundamental rights and fundamental freedoms that require the protection of personal data (see section 2.2 above). The legitimate interest is that the credit reference agency informs third parties about negative payment experiences and thereby protects against its own disadvantages.

2.5 Biometric Data

We utilise fingerprint technology to secure access to some areas, equipment and cabinets within our premises. Where appropriate to the services you supply to us, and subject to your consent, we process your fingerprint for the purpose of managing your access to the areas, equipment and/or cabinets to which the access controls have been applied. We also keep a log of the time and date of your access and the key(s) taken, which we use for the purpose of securing our premises. Such log data may be used, where relevant, during investigations and in connection with any complaints, claims and management of our contract with you.

The legal basis for the processing of your fingerprint data is your consent (UK GDPR Article 6(1)(a) and Article 9(2)(a)) and such consent will be collected and recorded by a consent form. The legal basis for our processing of data relating to the time and date of your access is our legitimate interest in protecting our employees, visitors, and property, as well as ensuring accountability. This is in accordance with the (UK GDPR Article 6(1)(f)).

3. Sources

We receive the personal data processed by us mainly in the context of our business relationship with you. We may also collect personal information about you from other sources (such as credit reference agencies, supplier references), which we will add to the information we already hold about you in order to help us improve our products and services, e.g., to improve and personalise the products / services which we are providing to you (under the GDPR, this purpose will not include marketing).

To the extent necessary for the provision of our services, as part of our business relationship or for the purposes set out above, we will process personally identifiable information obtained from other companies or from other third parties (eg credit bureaus, ad agencies). In addition, we may legitimately process, obtain, or acquire and process personal data obtained from publicly available sources (such as telephone directories, trade and association registries, civil registration registers, debtor directories, land registers, press, internet and other media).

4. Recipients or categories of recipients of your data

Your data will be processed by those with the necessary and relevant access within HARIBO.

A transfer of your data to third parties may occur to the extent permitted or required by law or as far as you have consented. We also share your data as necessary with service providers we use to provide and receive services. We limit the disclosure of data to what is necessary. As processors, these service providers are subject to contractual processing agreements and in accordance with GDPR Article 28, will only process your data in accordance with our instructions.

Here are the categories of recipients of your data:

- Affiliated companies within the Group, as far as they work for us as processors, e.g. in relation to internal IT services or, to the extent necessary for the provision of our services,
- Payment service providers and banks to collect outstanding payments from accounts or to pay reimbursement amounts,
- Call centers to respond to your requests and complaints,
- Agencies, print shops and lettershops that support us in the implementation of advertising measures, competitions, promotions, etc.,
- IT service providers, that for example store data, assist in the administration and maintenance of systems, and file archivers and destroyers,
- Logistics service providers to deliver goods, etc.,
- Credit reference agencies when undertaking a credit reference check,
- Collection agencies and legal advisers in asserting our claims,
- Public bodies and institutions as far as we are legally obliged to do so.

In addition, we may share your personal data with our Group, e.g., to affiliates who need this information to fulfill our contractual and legal obligations or based on our legitimate interests. These may be economic, administrative or other internal business purposes; this applies only insofar as your interests or fundamental rights and fundamental freedoms that require the protection of personal data do not prevail. In addition, we do not pass on your data to third parties.

5. Third country transfer

A transfer of data to countries outside the UK, EU or the EEA (so-called third countries) only takes place, as far as this is required by law (e.g., tax reporting obligations) or as required in the course of the performance of our contractual relationships, where you have given us consent or as neccessary as part of processing an order. If our service providers are, or use services that are, deployed in a third country, they are required to comply with the level of data protection in Europe in addition to our written instructions, for example by agreeing on EU standard contractual clauses, or on the basis of Binding Corporate Rules. Further information can be obtained by contacting us as set out in section 1 above.

6. Data Security

To ensure the security of data stored at HARIBO, appropriate technical and organisational measures have been implemented which also ensure the protection of data against unauthorised access, processing, or disclosure as well as accidental loss, alteration, or destruction. HARIBO has taken measures to ensure a level of protection appropriate to the processing risk in terms of the confidentiality, integrity, availability and resilience of IT systems, databases, etc. HARIBO also aims to secure confidentiality is implemented through access control and restrictions. Integrity is implemented through transfer control, input control and order control. Availability and resilience are also ensured by HARIBO through measures for availability and regular monitoring of such measures.

These technical and organisational measures are described in HARIBO's Information Security Directive which is available upon request. These are continuously adapted to reflect technical developments and organisational changes.

7. Duration of storage of your data

We process your data for the duration of our business relationship. This also includes the initiation of a contract (pre-contractual legal relationship) and throughout the execution of a contract.

In addition, we are subject to various storage and documentation requirements for example in relation to HMRC or health and safety. The deadlines for storage and documentation specified are up to 6 years beyond the end of the business relationship or the pre-contractual legal relationship.

In addition, we will store your data until the statute of limitations for any legal claims arising from our contractual relationship has expired, in order to refer to such data as evidence if necessary. This limitation period is usually 6 years.

If the data is no longer required for the fulfillment of contractual or legal obligations and rights, these will be deleted, unless their (limited) further processing is required in individual cases to fulfill the purposes listed in section 2 above. In such cases, we may also store and, if necessary, use your data after the termination of our business relationship or our pre-contractual relationship for a period consistent with such purposes.

If we process your fingerprint data, such data will be retained for the duration of our business relationship and three months thereafter. However, if you withdraw your consent to our processing of your fingerprint data we will delete such data as soon as practicable following our receipt of your consent withdrawal. Any access logs collected in respect of your access to our property and premises (including where linked to your fingerprint) will be retained for up to 18 months following collection.

8. Your Privacy Rights

In accordance with data protection legislation, you are entitled to the following rights as the person concerned, which you can exercise by using the contact details in section 1 above.

- **Right of access:** You are entitled at any time to request confirmation from us within the scope of Article 15 of the GDPR. To the extent that we process your data, you are also entitled under Article 15 of the GDPR to receive information about this data and certain other information (including processing purposes, categories of data, categories of recipients, planned storage period, your rights, the source of the data, the use of automated decision making and in the case of third country transfer the appropriate safeguards) and to obtain a copy of your data.

- **Right to rectification**: You are entitled, under Article 16 of the GDPR, to the rectification of inaccurate data and the completion of incomplete data relating to you (including by providing a supplementary statement).

- **Right to erasure:** You are entitled, under the Article 17 of the GDPR, to request that we delete your data without delay where it is no longer necessary for us to use it, you have withdrawn consent, or where we have no lawful basis for keeping it. Please be aware that we do not always need to comply with your request to the extent that the processing of the data is required as a result of, for example, (i) the exercise of the right to freedom of expression and information, (ii) the fulfillment of a legal obligation to which we are subject (e.g., statutory retention obligations) or (iii) the establishment, exercise, or defense of legal claims.

- **Right to restriction of processing:** You are entitled to request under Article 18 of the GDPR that we limit the processing of your data where you have asked for it to be erased or where you have objected to our use of it.

- **Right to data portability:** In certain circumstances, you may be entitled, under the Article 20 of the GDPR, to demand that we provide you or a third party with the data relating to you provided to us in a structured, commonly used, and machine-readable format.

- **Right to object:** In certain circumstances, you are entitled, under Article 21 of the GDPR, to object to the processing of your data. For example, where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground. The right to object exists only in limited circumstances. In addition, we may have legitimate grounds which may preclude termination of processing. We will inform you to the extent that, despite your opposition, we have legitimate grounds (in accordance with the GDPR) to process your data.

- **Revocation of consent:** To the extent we rely on consent as the legal basis for processing your data, you have the right at any time to revoke such consent. Most of the time, we won't need your consent to use your data as we will be using it only to fulfil our obligations and exercise our rights under our contract (as set out above). If you have given your consent and you wish to withdraw such consent, we will inform the recipient of the data accordingly and refrain from processing the data for the purposes covered by the consent in the future. For documentation purposes, we will store information about this withdrawal of consent.

- **Right to complain:** In addition to the listed rights above, you have the right to complain to us by contacting us in accordance with section 1 above to the supervisory authority in accordance with Article 77 of the GDPR if you believe that the processing of your data is not lawful. The address of the supervisory authority responsible for our company is:

  Information Commissioner's Office
  Wycliffe House
  Water Lane
  Wilmslow
  Cheshire, SK9 5AF

  Telephone: +44 (0) 1625 545 745
  Fax: +44 (0) 1625 524 510

  Email: england@ico.org.uk

  However, we recommend that you always file a complaint with our data protection coordinator, at the contact details given in section 1 as we may be able to address your concern.

  Your requests for the exercise of your rights should, if possible, be addressed in writing to the address given above or directly to our data protection coordinator.

9. Scope of your obligations to provide us with your data

In light of the grounds for processing your data as outlined in this privacy policy, we will generally not be able to conclude or execute the contract without such data at the outset. This may also apply to data required later in the business relationship. If we request further data from you, which we require your consent to process, you will be informed about the voluntary nature of the information separately.

10. Existence of automated decision-making in an individual case (including profiling)

Automated decision-making takes place when an electronic system uses data to make a decision without human intervention. You have the right not to be subject to automated decisions that will create legal effects or have a similar significant impact on you, unless you have given us your consent, it is necessary for a contract between you and us or is otherwise permitted by law. You also have certain rights to challenge decisions made about you. We do not automate decision-making procedures according to Art. 22 GDPR or profiling. If we should use such a procedure in individual cases in the future, we will inform you about this separately.

11. Keeping you up to date

We reserve the right to change this Privacy Policy at any time. Where appropriate, we shall notify you of these changes by the issuing of a revised version, by email

Latest version: As of May 2025.