HOKODO

Hokodo Privacy Policy

1. Introduction

This document explains how Hokodo (collectively "**Hokodo**", or "**we**" or "**us**") protects the personal information of our Merchants, Customers and other parties, including how we ensure that personal information is processed in accordance with the General Data Protection Regulation (GDPR) and the Data protection Act 2018 (UK).

We help suppliers of goods or services ("**Merchants**") to offer credit terms to businesses purchasing those goods or services ("**Customers**"). To do this, we offer one or more of the following solutions to Merchants (the "**Services**"):

- **Credit and/or Fraud assessment**: we evaluate orders to determine whether a given transaction can be offered on credit terms. This may include an assessment of the Customer's creditworthiness as well as the likelihood that the transaction is fraudulent
- **Credit and/or Fraud protection**: in certain circumstances we protect Merchants against financial losses arising from non-payment by Customers due to insolvency, unwillingness to pay, or fraud. This protection may be in the form of an insurance policy, or through a finance contract whereby we advance funds to the Merchant against the Customer payment that is due, and where those funds are not repayable in the event of a Customer default
- **Financing**: We provide financing to Merchants so that they can get paid before the Customer has settled the transaction
- **Debt Collection**: We collect payment from Customers or, in the case of severely overdue payment, arrange for a 3rd party debt collection agency to recover unpaid balances

We focus exclusively on business-to-business transactions. As such, the Customers of our Merchants are normally businesses, and so the data we process is mostly that of companies rather than individuals. Some notable exceptions are when we process information regarding:
i) sole traders, who trade as an individual rather than as a company;
ii) the details of individual employees at Merchants, Customers or our distribution partners
iii) individuals associated with these companies on public registers such as directors, officers and significant shareholders.

2. What personal information do we process and why?

The Personal Information we process differs according to our relationship with that party.

Merchants

In order to provide the Services to the Merchants, we process information such as:

- **Contact details** of the individuals with whom we interact to do business, including: address, telephone number, email address and contact history
- **Transaction history** which Merchants share with us, including both their historical sales and the details of future sales which they would like us to finance or insure
- **Name, address, date of birth and identity documents** of the beneficial owners and directors or the individuals exercising significant control over the Merchant, plus any associated video verification, which we are required to collect by the relevant authorities for the purposes of combating financial crime
- **Information about the financial solvency of the Merchant**, including information the Merchant shares with us and information which we source from 3rd party sources such as public registers and Credit Reference Agencies ("**CRAs**") and Fraud Prevention Agencies ("**FPAs**"). For more information on our use of CRAs and FPAs, see section 5.
- **Recorded telephone conversations** if Merchants call us or if we call Merchants, if we inform them about this at the start of the call

This information is processed for one of several purposes:

- To enable us to provide operational and administrative support the the Merchant
- To enable us to offer quotes to the Merchant, or to administer contracts of insurance or finance agreements with the Merchant
- To enable us to manage our credit exposures to the Merchant
- To enable us to screen for different forms of financial crime including fraud, money laundering, and breach of sanctions rules
- To enable us to train our algorithms and improve the accuracy with which we can credit score companies and predict fraud

Subject to their consent, contact details of Merchants and their employees may also be used for our own marketing purposes, for example to notify Merchants of a new product that we think they might be interested in.

Customers

In order to provide the Services to Customers, we process information such as:

- **Contact details** of the individuals (typically employees) making purchases on behalf of Customers or processing payments, including: name, gender, telephone number, email address, business address and contact history
- **Details of the purchase** to be financed or insured, including the items being purchased, the shipping address, and the shipping or tracking number
- **Transaction history** of the Customer including: transaction value, issue date, due date, paid date etc.
- **Information about the financial solvency of the Customer**, including information which is shared with us by the Customer directly, or via the Merchant, and information which we source from 3rd party sources such as public registers, CRAs and FPAs. For more information on our use of CRAs and FPAs, see section 5.
- Any **non-payment history** of the Customer, including the status of any debt collection
- **Information about the device** used by Customers to undertake or confirm a transaction, such as the IP address, language and browser settings, operating system etc. as well as information about the Customer's behaviour on our website
- Details of **directors and significant shareholders** of the Customer, as obtained from publicly-available sources such as Companies House.
- **Recorded telephone conversations** if Customers call us or if we call Customers, if we inform them about this at the start of the call
- **Payment information** - we collect bank account information if Customers choose to pay by Direct Debit. We do not collect credit card information, as this is handled directly by our payment processors.
- **Identity documents**: In certain circumstances, we may ask either the employee of a Customer placing an order, or a director of the Customer to complete an identity verification as a fraud prevention measure. In this case we process the video recording or identity documents they upload such as their passport or proof of address.

This information is processed for one of several purposes:

- To enable us to provide operational and administrative support the the Customer
- To enable us to calculate a credit score for the Customer or to assess their creditworthiness in order to offer payment terms
- To enable us to assess the Customer's order for fraud risk, and to prevent

fraudulent misuse of the Customer's identity
- To enable us to screen for different forms of financial crime including money laundering, and breach of sanctions rules
- To enable us to offer quotes to the Merchant so that the Merchant can offer payment terms to the Customer
- To administer contracts of insurance or finance agreements with the Merchant, which in turn permit the Merchant to provide payment terms to the Customer
- To enable us to train our algorithms and improve the accuracy with which we can credit score companies and predict fraud

Subject to their consent, and our contract with Merchants, contact details of Customers may also be used for our own marketing purposes, for example to notify Customers of a new product that we think they might be interested in.

Business partners

We hold and process the contact details of our business partners with whom we interact to do business. We may also contact our business partners for our own marketing purposes.

Employees and Job Applicants

In order to facilitate the day-to-day running of our business, we hold personal information for all our employees, such as: bank details, identification documents, contact details etc. As part of our recruitment process we receive the CVs of job applicants, which include contact details as well as other personal data (eg. date of birth).

Website visitors

Visitors to our public website do not have their personal information collected unless they choose to fill out a form giving us permission to contact them. However, we do process some non-personally identifiable data, such as: the IP address, language and browser settings, operating system etc. For further information, please consult our Cookie policy.

3. Lawful basis for processing personal information

The legal bases upon which we process and hold personal information are:

- **Performance of contract**: in order to provide an insurance quote or an offer of financing; or to administer a contract of insurance or a financing contract, it is necessary for us to process data about Merchants and Customers.
- **Legitimate interest**: we process personal information of certain Customers on the basis of legitimate interest, for example to:
  i) characterise the risk profile of the Customer
  ii) collect payment from the Customer
  iii) identify and prevent fraud
  We ensure that the processing performed for this purpose is necessary for fulfilling our legitimate interest, and that our interest outweighs the Customer's interest in not having their personal data processed for this purpose.
- **Consent**: when marketing to Insureds or business partners, we obtain the active consent of these parties and they are given the clear option to opt out at any time.
- **Legal obligation**: we are occasionally compelled to process the personal information of parties with whom we interact or to share their data with regulatory authorities in order to comply with regulatory or legal requirements, such as for the prevention of money laundering or combating tax fraud or the financing of terrorist activities.

4. Retention period

Unless otherwise instructed, we will retain personal information for a reasonable and necessary time taking into account the purposes of the processing and the legal and regulatory requirements. We will always destroy personal

information within ten years of the termination of a contract.

Our standard data retention periods are as follows:

- Merchant contact and contractual information, and details of transactions which we have financed or insured: 10 years after the expiration of our contract with the Merchant, or after the date of the transaction
- Details of transactions which we have quoted on but not insured or financed: 3 years after the quote date
- Any documents and data confirming/justifying validity of a transaction will be retained for at least 8 (eight) years from the conclusion of the transaction
- Details of the directors and beneficial shareholders of companies: 7 years from the end of the directorship or from the record of beneficial shareholding
- Contact details of our distribution partners: 3 years after the end of the distribution agreement
- Contact details used for payment collection: 3 years if payment collection is successful, 10 years if the payment collection is unsuccessful
- Employee records: 10 years from termination of employment
- Job applicant records: 3 years from the date of the application
- Call recorded for quality monitoring and internal training: 6 months after a call date.

5. Cooperation with Credit and Fraud agencies

In certain cases we may share information about Customers or Merchants with Credit Reference Agencies ("**CRAs**"). We do this in order to assess the creditworthiness of the Customer or Merchant.

We may share the following information with CRAs:

- For Customers who are companies: Company Name, trading address, bank account number and sort code
- For Customers who are sole traders, partnerships or other unregistered businesses, or for companies that have not published financial reports: Name of the sole trader/partners/director, gender, address, date of birth, phone number, bank account number and sort code

The CRAs will then provide us with any solvency data concerning the Customers and their financial associates held in their database, including credit scores calculated using their own statistical techniques. In addition they may send us confirmation of the validity of the customer information we have submitted.

We only ever conduct "soft" credit searches on Customers, meaning that our search never affects Customers' credit records.

We may also share information about the payment performance of Merchants or Customers whose purchases we have insured or financed with CRAs. This may include details of outstanding balances, payments made, and any default or failure to make payment when it falls due. These records may remain on the CRA's files in line with their data retention policies, and this information may affect future credit decisions which are made by the CRA's other Customers.

For German self employed businesses and small business owners, we may use the information you provide to us to conduct a credit rating/solvency check with Creditreform Boniversum GmbH, Hellersbergstr. 11, 41460 Neuss, Germany. Creditreform sends us your personal address data and solvency data stored in its databases including score values calculated using actuarial techniques, insofar as we have credibly demonstrated our legitimate interest therein. The calculation of the score value uses address data amongst other things.

We may share the Customer information listed in Section 2 with Fraud Prevention Agencies ("FPAs"). We do this in order to protect the Customer or Merchant from Fraud, and to prevent criminal activities.

The personal information we collect from Customers may be shared with FPAs who will use it to prevent fraud and money laundering and to verify Customers' identity. If fraud is detected, Customers could be refused certain services, finance or employment. Further details of how Customers' information will be used by us and these FPAs, along with Customers' data protection rights, can be found here.

We work with the following CRAs and FPAs:

- Experian
- Duedil
- Ellisphere
- Boniversum
- E-Informa
- Lexisnexis
- CIFAS

6. Third party transmission

In order to conduct our business, we need to share information on Merchants and Customers with selected third parties, such as:

- Other companies in the Hokodo group
- The insurers who underwrite our insurance products, and associated insurance intermediaries (eg. brokers, FCA/ORIAS-registered companies) and reinsurers,
- The financers who finance the credit we provide to Merchants,
- Debt collection agencies,
- Claims adjusters,
- Legal or regulatory bodies, the police or tax authorities where we are required to do so in order to comply with diverse regulations such as to prevent money laundering or the financing of terrorist activities, and
- Service providers, such as: IT platforms, payment processing providers, lawyers, other specialised consultants and marketing and communication firms.

We may also need to share certain Customer data with the Merchant from whom they made their purchase to enable the Merchant to fulfil the purchase.

We strictly limit the disclosure of personal information to third parties to that which is required for the fulfilment of the agreed purpose and nothing more.

The data we process may be transferred outside the EEA as part of interactions with these third parties. In such cases, we have safeguards in place including contractual clauses to ensure third parties meet the standards required by EU law.

If you pass us personal information regarding another party, it is your responsibility to ensure that, where it is necessary to do so,
i) you have told the individual who we are and what personal information we process (as set out in this Privacy Policy); and
ii) you have permission from this individual to pass us their personal information (including any sensitive personal data).

7. How your personal data is protected

Any data held by us is stored encrypted on our servers. Access to personal information is only granted to persons for whom it is necessary for the performance of their tasks. These persons are contractually bound to strict professional discretion. We pay particular attention to the protection of privacy and employ industry-standard technical and organisational measures against loss, destruction, access and alteration or distribution of personal information by unauthorised persons. It should, however, be noted that the processing and transmission of data is inherently subject to security risks.

Our website may contain links to third party sites (eg. social media) whose terms of use do not fall within the scope of this Privacy Policy and should be consulted to find out how they respect your privacy.

8. Your rights

In accordance with GDPR, the following rights exist with respect to Personally Identifiable Information ("**PII**"):

- Right to be informed (that PII is being held and what we do with it),
- Right of access (to view your PII),
- Right of rectification (to ask us to change the PII if you believe it is incorrect),
- Right to erasure (to ask us to delete your PII if we no longer need it, if you believe we have obtained the data unlawfully or if you have removed your consent for particular activities),
- Right to restriction (to stop us from doing particular things with your PII),
- Right to portability (to pass the PII on to another party),
- Right to object (to ask for your data not to be used for direct marketing or for "legitimate interests"), and
- Rights related to automatic decision-making, including risk profiling (to have a human review any decision that has been made about you by our risk profiling and pricing algorithms).

Please contact us via support@hokodo.co if you wish to discuss or begin the process of exercise of any of the above rights.

You also have the right to lodge a complaint with a supervisory authority ICO, or CNIL, or State Data protection inspectorate. An overview of the Data Protection Authorities may be found http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

9. Modification of this privacy policy

We may adapt this Privacy Policy at any time, and the changes will be applicable at the time of publication on our website. We therefore advise you to consult the most recent version of this document.

10. Entities

In this policy, Hokodo, as a data controller, refers to the Hokodo entity with which you are communicating. Otherwise, it refers to the entity that corresponds to your domicile, which is the country of your residence (if you are an individual) or the place where you are incorporated (if you are a company, corporation, or other legal entity).

Hokodo entity	If Client is domiciled in
Hokodo Services Ltd	UK
Hokodo SAS	France, Spain, Belgium, Netherlands
Hokodo UAB	Any country or territory outside of the UK, France, Spain, Belgium, Netherlands

11. Contact details

To contact us with any questions about this policy, or to exercise any of your rights as a Data subject please email us at support@hokodo.co.