globalpayments

Merchant Data Processing Notice

of GP Payments Acquring International GmbH

This Merchant Data Processing Notice ("Notice") applies if you are entering into an agreement with GP Payments Acquiring International GmbH, ("GP") for the provision of card payment processing and other products and services made available by GP, including through accessing the GP Marketplace or other GP sites.

When we refer to "you" or "Merchant" in this Notice, we refer to the entities who provide us with personal data in order to procure these services. In the case of sole traders, partnerships, and other unincorporated customers, this will be the individuals who own the business, and for corporate customers, this will mean any directors, officers, shareholders, or other parties responsible for the operation of the business whose data we collect. In all cases, this will include any joint applicants or guarantors whose personal data we process.

1. Who we are and how to contact us.

GP Payments Acquiring International GmbH, Elsa-Brändström-Str. 10–12, 50668 Cologne, Germany is a data controller of your personal data, which means information that is about you or from which we can identify you. This Notice describes how we deal with your personal data.

We are the data controller of this personal data under relevant data protection laws because in the context of our business relationship with you, we decide how and why it is processed in the ways explained in this Notice. When we use terms such as "we," "us" and "our" in this Notice, we mean GP.

Our Data Protection Officer can be contacted at any time, including if you have queries about this Notice or wish to exercise any of the rights mentioned in it, by emailing dpo@globalpay.com or by mail to GP Payments Acquiring International GmbH, Elsa-Brändström-Str. 10–12, 50668 Cologne, Germany.

2. Where do we get your personal data?

We will generally collect your personal data from the following sources:

- from you directly.
- from our Partners with whom you may have a contractual relationship.
- from sources such as Fraud Prevention Agencies and Credit Reference Agencies.
- from other members of our Group if you already have a product with them, from Card Schemes or from business information solutions.

Some of the personal data may also have originated from publicly accessible sources.

3. What kinds of personal data about you do we process?

We process the personal data that you provide to us during the Merchant application and onboarding process as well as during your ongoing relationship with us.

The personal data includes:

- Your title, full name, your contact details (business / home address, email address, telephone numbers);
- Data you provide to us to verify your identity, such as copies of passports, driving licences or utility bills;
- Data arising from your use of our services (for example, data on the volume of transactions, and transaction execution data;
- Information regarding our interactions with you, including, but not limited to, customer service requests, online and telephone communications;
- Device Information and other unique identifiers, including device / browser identifiers, internet protocol (IP) address, cookies, beacons, pixel tags, or similar unique identifiers;
- Personal data that we obtain from Fraud Prevention Agencies; Personal data about your credit history that we obtain from Credit Reference Agencies; and
- Where relevant, personal data about any guarantor that you provide in any application.

If you make a joint application or provide a guarantor, we will also collect the personal data mentioned above about that person. If you are a corporate entity, we will collect the personal data mentioned above about the directors, shareholders and other managers whose names are provided to us by you. You must show this Notice to the other applicant and ensure they confirm that they know you will share it with us for the purposes described in it.

4. What are the legal grounds for our processing of your personal data?

Data protection laws require us to explain what legal grounds justify our processing of your personal data (this includes sharing it with other organisations). For some processing, more than one legal ground may be relevant. Here are the legal grounds that are relevant to us:

1. Processing necessary **to perform our contract with you or for taking steps prior to entering into it**, in accordance with Art. 6(1)(b) GDPR, such as:
   - Verifying your identity.
   - Administering, managing your services and updating your records.
   - Providing you with the requested services or products (which may include sharing your data with 3rd Parties).
   - Providing you with customer service via telephone, customer chat, via social media platforms or other online channels of communication; and
   - Sharing your information with the following entities to facilitate the provision of our services to you:
     - the Card Schemes such as Mastercard, Visa, or any applicable card association or organisation including, without limitation any parent, affiliate, subsidiary, or successor, of any of them.
     - Qualified Security Assessors, or other providers, to verify your Payment Card Industry Data Security Standard (PCI DSS) compliance and compliance with your security obligations under our agreement with you.

2. Where we consider that it is appropriate for us to do so for processing that is necessary **for our legitimate interests or in some cases, that of a 3rd party**, in accordance with Art. 6(1)(f) GDPR including:
   - To administer and manage our relationship and your services and to keep appropriate records;
   - To improve our products and services, by reviewing which products you choose, the frequency and type of use, and to evaluate their performance;
   - To adhere to guidance and best practice under the regimes of governmental and regulatory bodies;
   - To administer good governance for us and other members of our Group, and for audit of our business operations including accounting;
   - To carry out searches at Credit Reference Agencies;
   - For fraud prevention and debt recovery;
   - To carry out monitoring (including of telephone calls, and where consent is not required by applicable law) as required for security and regulatory purposes;
   - For market research, product surveys, analytics and statistics development.
   - To determine your eligibility for additional products or services that we believe may be of interest to you (which may include sharing your data with 3rd Parties);
   - For direct marketing of GP products and partnership offers, (where consent is not required by applicable law), to inform customers about updates to our existing products, the launch of new products as well as products which are offered together with or by our partners; and
   - To maintain the safety and security of our systems, employees and premises.

3. Processing necessary **to comply with our legal obligations**, in accordance with Art. 6(1)(c) GDPR:
   - For compliance with laws that apply to us;
   - For establishment, defence and enforcement of our legal rights or those of any other member of our Group.
   - For activities related to the prevention, detection, and investigation of crime;
   - To carry out identity, anti-money laundering checks, and other relevant checks with Fraud Prevention Agencies pre-application, at the application stage, and periodically after that;
   - To respond to requests from you to exercise your rights under data protection laws;
   - When we share your personal data with these other people or organisations:
     - Your guarantor (if you have one).
     - Law enforcement agencies and governmental and regulatory bodies; or
     - Courts and other organisations where that is necessary for the administration of justice, to protect vital interests and to protect the security or integrity of our business operations.

4. Processing with your **consent** where required by applicable law, in accordance with Art. 6(1)(a) GDPR:
   - To send you direct marketing communications;
   - Share your information with a 3rd party;
   - To collect information via cookies or similar technologies; and
   - For identity verification purposes: In order to provide you with certain services, we are legally obliged to verify your identity. This verification may be through documentary, photographic and / or biometric means and is based on the technology of comparing facial biometric features and a photo from an identity document. Once the identity verification process is completed only the result of that comparison (match or mismatch) will be retained. Biometric data is considered to be a “special category of data” when used for verification purposes and therefore, the legal basis for processing is your consent. Once you have completed the identification process, your personal data will be retained only for as long as required to fulfil our legal obligations.

5. Personal data processing as part of providing the GP products and services

When you choose the use the following GP products or services, we process your personal data (which may include a transfer to a 3rd party) as described below:

Product / Service	Personal data processed	Legal Basis
GP Tap on Mobile (TOM)	Merchant information, including merchant / company name, address, identification information, Merchant ID number, and User ID (where relevant).	Performance of the contract between you and GP in accordance with Art. 6(1)(b) GDPR.
GP Point of Sale (POS)	Merchant information, including merchant / company name, address, identification information, Merchant ID number, and User ID (where relevant).	Performance of the contract between you and GP in accordance with Art. 6(1)(b) GDPR.
GP Webpay	Merchant information, including merchant ID, identification information, onboarding information.	Performance of the contract between you and GP in accordance with Art. 6(1)(b) GDPR.
GP Payment Analytics	Merchant information, including merchant / company name, address, Merchant ID number.	Performance of the contract between you and GP in accordance with Art. 6(1)(b) GDPR.
GP Predictive Analytics	Merchant information, including merchant / company name, address, Merchant ID number.	Performance of the contract between you and GP in accordance with Art. 6(1)(b) GDPR.
Customer Demographics	Merchant information, including merchant / company name, address, Merchant ID number. This information is also shared with our partner (MasterCard) in order to provide the requested demographics information.	Performance of the contract between you and GP in accordance with Art. 6(1)(b) GDPR.
Flexible Financing	Merchant information, including merchant / company name, address, business ID number. GP shares this information with the partner (Liberis) for the purposes of determining your eligibility for the financing offer. If you use the Create Digital API, we will also process the full name and date of birth of all directors / or employees who own more than 25% of the shares of the Merchant business.	This processing is based on our legitimate interest to provide customers with relevant information and targeted offers in accordance with Art. 6(1)(f) GDPR. To object to our processing of your data for this purpose, please contact dpo@globalpay.com Performance of the contract in accordance with Art. 6(1)(b) GDPR.
Competitive Benchmark	Merchant information, including merchant / company name, address, Merchant ID number). The above information is also shared with our partner (Mastercard) in order to provide the requested benchmarking information.	This processing is based on our legitimate interest to provide you with relevant and targeted offers, according to Art. 6(1)(f) GDPR. Performance of the contract between you and GP in accordance with Art. 6(1)(b) GDPR.

5.1 GP Partner products

When you use the following products available in the Marketplace that are provided to you via 3rd Parties or GP Partners, GP is an intermediary in these relationships and the data processing is subject to the terms, conditions, and privacy practices of those 3rd Parties. GP may share your data with these 3rd Parties in order to facilitate the provision of the services which you have requested.

3rd Party / Service	Personal Data processed	Legal Basis
Alphabet Inc. / Google Business Profile	Merchant information, including merchant / company name, merchant ID, address, and email address.	Performance of the contract in accordance with Art. 6(1)(b) GDPR.
Alphabet Inc. / Google Ads	Merchant information, including merchant / company name, merchant ID, email address.	Performance of the contract in accordance with Art. 6(1)(b) GDPR.

For information on how these 3rd Parties process your personal data, please visit their websites as applicable.

6. How and when can you withdraw your consent?

Where processing of your personal data is based on your consent, you have the right to withdraw that consent for future processing at any time. You can do this by contacting us by email via dpo@globalpay.com or by visiting the Merchant Marketplace or, for direct marketing communications, from the unsubscribe link in any marketing communication.

The consequence might be that we cannot send you some marketing communications, or that we cannot consider special categories of personal data or provide you with certain Services. Please note that if you opt out of receiving marketing-related communications from us, we may still send you administrative, transactional, or account information messages, from which you cannot opt out.

7. Is your personal data transferred outside the European Union?

As our affiliate companies are located around the globe, your personal information may be transferred to and stored in another country outside of the country in which you reside, including in the United States, which may be subject to different standards of data protection than your country of residence.

Subject to your consent if required by applicable law, we may appoint an affiliate company to process personal information in a service provider role. We will remain responsible for that company's processing of your personal data pursuant to applicable data privacy laws.

We take appropriate steps to ensure that transfers of personal information are in accordance with applicable law, are carefully managed to protect your privacy rights and interests and limited to countries which are recognized as providing an adequate level of legal protection or where alternative adequate arrangements are in place to protect your privacy rights.

For more information about suitable safeguards and (where relevant) how to obtain a copy of them or to find out where they have been made available, you can contact our Data Protection Officer using the email details above.

8. With whom do we share your personal data?

- With Members of the Global Payments Group to facilitate entering into a contractual relationship with you and the provision of our products and services to you.
- With our partners and 3rd parties, including those businesses who provide services directly to Merchants to facilitate requested products and / or services.
- The sales company or organisation who referred or introduced you to us.
- Your guarantor (if you have one).
- The Card Schemes.
- Debt recovery agencies.
- Credit reference and Fraud prevention agencies.
- Our legal and other professional advisers, auditors and actuaries.
- Financial institutions and trade associations.
- Governmental and regulatory bodies
- Qualified security assessors, or other providers, to verify your PCI DSS compliance and compliance with your security obligations under our agreement with you.
- Market research organisations who help us to develop and improve our products and services.
- Other organisations and businesses who provide services such as back up and server hosting providers, IT software and maintenance providers, document storage providers and suppliers of other back-office functions.
- Buyers and their professional representatives as part of any restructuring or sale of our business or assets.

9. How we share your personal data with Credit Reference Agencies

In order to process your application, we will perform credit and identity checks on you with one or more Credit Reference Agencies ("CRAs"). To do this, we will supply your personal data to CRAs, and they will give us information about you. CRAs will supply to us both public (including the electoral register) and shared credit, financial situation and financial history information and fraud prevention information.

We will use this information to:

- Assess your creditworthiness and whether you can afford to take the product;
- Verify the accuracy of the data you have provided to us;
- Prevent criminal activity, fraud and money laundering;
- Trace and recover debts.

We will continue to exchange personal data about you with CRAs while you have a relationship with us.

When CRAs receive a search from us, they will place a search footprint on your credit file that can be seen by other people who carry out searches.

This information about CRAs is condensed. GP will identify the CRA used in relation to your personal data on request, by emailing our Data Protection Officer as detailed above.

Please note that the processing of your personal data within these agencies is governed by the policies adopted by the relevant agencies. You can contact the CRAs directly by visiting their websites to obtain a copy of your information from them.

- Experian Germany: www.experian.de
- SCHUFA Holding AG: www.schufa.de

10. How we share your personal data with Fraud Prevention Agencies

If you provide false or inaccurate information or fraud is suspected or identified, your details will be passed to Fraud Prevention Agencies. If we terminate or suspend service under our agreement with you, we may pass details of the reason it is terminating or suspending service under the agreement together with details of your business, including without limitation the names and addresses of the principal proprietors or directors, to fraud prevention databases operated by Card Schemes. The types of reason that may be notified to Card Schemes include, but are not limited to, circumstances such as insolvency, breach of our agreement or excessive levels of fraudulent transactions or Disputes.

We, and Fraud Prevention Agencies, will use this information to prevent fraud and money laundering, and to verify your identity. We and Fraud Prevention Agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

Fraud Prevention Agencies can hold your personal data for different periods of time, depending on how that data is being used. You can contact them directly for more information. If you are considered to pose a fraud or money laundering risk, your data can be held by Fraud Prevention Agencies for up to six years from its receipt.

A record of any fraud or money laundering risk will be retained by the Fraud Prevention Agencies and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, you can contact the appropriate Fraud Prevention Agency.

This information about Fraud Prevention Agencies is condensed. GP will identify the Fraud Prevention Agencies it uses on request by emailing our Data Protection Officer as detailed above. You can contact the Fraud Prevention Agencies directly to obtain a copy of your information from them. Information held may differ so you may wish to contact them all.

11. How long do we retain your personal data?

We retain the personal data we collect for different periods of time depending on what it is and how we use it. In some contexts, we will provide additional information about retention as you use the services. When we collect personal data, we will retain it only for as long as is necessary to complete the legitimate business or legal purposes for which we collected it. The criteria used to determine our retention periods include:

- The length of time we have an ongoing relationship with you and provide services to you, for example, for as long as you continue to use our services, and the length of time thereafter during which we may have a legitimate need to reference personal data to address issues that may arise.
- Whether there is a contractual obligation to which we are subject, for example, our contracts with you may specify a certain period of time during which we are required to maintain the data.
- Whether there is a legal obligation to which we are subject, for example, certain laws require us to keep records of transactions for a certain period of time before we can delete them; and
- Whether retention is advisable to preserve our legal position, such as in regard to applicable statutes of limitations, litigation or regulatory investigations.

12. What are your rights under data protection laws?

You have certain rights in relation to the processing of your personal data, some of which may not apply in all circumstances. To learn more or to exercise your rights, you can contact our DPO via dpo@globalpay.com.

- The right to be **informed** about our processing of your personal data;
- The right to have your personal data **corrected if it is inaccurate** and to have **incomplete personal data completed**;
- The right **to object** to processing of your personal data, where we are relying upon legitimate interest to process data;
- The right **to restrict processing** of your personal data;
- The right **to have your personal data erased** (the 'right to be forgotten');
- The right to **request access** to your personal data and to obtain information about how we process it;
- The right to **move, copy or transfer your personal data** ('data portability'); and
- Rights in relation to **automated decision making that has a legal effect or otherwise significantly affects you**.

You have the right to complain to your country's data protection authority if you believe that our processing does not comply with applicable data protection laws.

If you wish to exercise any of these rights against the Credit Reference Agencies, the Fraud Prevention Agencies, or a broker or other intermediary who is a data controller in its own right, you should contact them separately.

13. Data Anonymisation and Use of Aggregated Information

Your personal data may be converted into statistical or aggregated data, which cannot be used to re-identify you. It may then be used to produce statistical research and reports. This aggregated data may be shared and used in all the ways described in this Notice.

This document was last issued in **July 2024** and may be amended from time to time. Updated versions will be posted on our website as detailed above.