

Merchant Data Processing Notice

This Merchant Data Processing Notice (“Notice”) applies if you are entering into an agreement with Global Payments Ltd trading as Global Payments (“GPN”) for the provision of Card Processing Services (“Services”). When we refer to “you” or “Merchant” in this notice, we refer to the individuals who provide us with Personal Data in order to procure these Services. In the case of sole traders, partnerships and other un-incorporated 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.

References to Card Schemes, means MasterCard, Visa, or any applicable card association or organisation (for example, Discover Global Network, JCB and UPI), including without limitation any parent, affiliate, subsidiary, or successor, of any of them.

1. Who We Are and How to Contact Us and Our Data Protection Officer

Global Payments Ltd of Ground Floor, Continental Business Centre, Old Railway Track, Santa Venera, SVR 9018 is a Data Controller of your Personal Data. This 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 GPN.

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@gpe.cz

Because we are a global company, your Personal Data may be shared with or processed by other members of our Group.

In this Notice we mention the use of Fraud Prevention Agencies and Credit Reference Agencies in sections 7 and 8. Please read these sections carefully and contact those organisations if you have questions about how they use your Personal Data.

2. Where Do We Get Your Personal Data?

We will generally collect your Personal Data from you directly.

In addition, we obtain your Personal Data and other sources such as Fraud Prevention Agencies and Credit Reference Agencies. Some of your Personal Data may come from other members of our Group if you already have a product with them or from Card Schemes or from Search Engines such as Accuity.

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 application process, as well as data we obtain from any sales agent who has third party sources to verify your Personal Data, including Credit Reference Agencies. The Personal Data includes:

- Your title, full name, your contact details, including for instance your email address, home and mobile telephone numbers;
- Your home address, correspondence address (where different from your home address) and address history;
- Records of how you have contacted us and, if you get in touch with us online, details such as your mobile phone location data, IP address and MAC address;

- Data you provide to us to verify your identity, such as copies of passports, driving licenses or utility bills;
- Personal Data that we obtain from Fraud Prevention Agencies (see the section on 'Fraud Prevention Agencies' below);
- Personal Data about your credit history that we obtain from Credit Reference Agencies, including data that originates from local authorities (electoral roll), the **Registry of Companies**, other lenders and providers of credit (who supply data to the Credit Reference Agencies), court judgments decrees and administration orders made publicly available through statutory public registers (see the section on 'Credit Reference Agencies' below);
- Where relevant, data about any guarantor that you provide in any application;
- Your management and use of the Services.

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 (Including When We Share It With Others)?

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 for the Services or for taking steps prior to entering into it:**
 - a) Verifying your identity;
 - b) Administering and managing your Services and updating your records; and
 - c) When we share your information with:
 - the Card Schemes.
 - 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.
 - Global Payments Europe in the Czech Republic
 - HSBC Bank Malta p.l.c. as our Data Processor.
- 2) Where we consider that it is appropriate for us do so, processing necessary **for the following legitimate interests**, which apply to us and, in some cases, other organisations (who we list below) are:
 - a) Administering and managing our relationship and your Services and keeping appropriate records;
 - b) To improve our products and services, by reviewing which products you take up and use and the frequency and type of use you make of the Services, and to test their performance;
 - c) To adhere to guidance and best practice under the regimes of governmental and regulatory bodies such as the Malta Financial Services Authority (MFSA), the Financial Intelligence Analysis Unit (FIAU), and the Information and Data Protection Commissioner's Office (IDPC);
 - d) To administer good governance for us and other members of our Group, and for audit of our business operations including accounting;
 - e) To carry out searches at Credit Reference Agencies;
 - f) To carry out monitoring (including of telephone calls) and to keep records;
 - g) For market research and analysis and developing statistics;
 - h) To provide the Dynamic Currency Conversion functionality;
 - i) When we share your Personal Data with these other people or organisations:
 - Your guarantor (if you have one);
 - Members of our Group;
 - The Card Schemes;
 - The sales company or organisation who referred or introduced you to us;
 - Debt recovery agencies;

- Our legal and other professional advisers, auditors and actuaries;
 - Financial institutions and trade associations;
 - Governmental and regulatory bodies such as MFSA, FIAU and IDPC
 - Qualified Security Assessors, or other providers, to verify your PCI DSS compliance and compliance with your security obligations under our agreement with you;
 - Other organisations and businesses who provide services to us 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;
 - Fraud Prevention Agencies;
 - Credit Reference Agencies;
 - Market research organisations who help us to develop and improve our products and services: and
 - Other organisations and businesses, who provide services directly to Merchants to enable transaction processing.
- 3) Processing necessary **to comply with our legal obligations**
- a) For compliance with laws that apply to us;
 - b) For establishment, defence and enforcement of our legal rights or those of any other member of our Group;
 - c) For activities relating to the prevention, detection and investigation of crime;
 - d) To carry out identity checks, anti-money laundering checks, and checks with Fraud Prevention Agencies pre-application, at the application stage, and periodically after that;
 - e) To carry out monitoring and to keep records;
 - f) To deal with requests from you to exercise your rights under Data Protection Laws;
 - g) When we share your Personal Data with these other people or organisations:
 - Your guarantor (if you have one);
 - Fraud Prevention Agencies;
 - Debt recovery agencies;
 - Law enforcement agencies and governmental and regulatory bodies such as MFSA, the FIAU and IDPC; and
 - Courts and to 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**:
- a) For direct marketing communications;
 - b) When you consent for us to share your information with a third party; and
 - c) Where information has been gathered via cookies or similar technologies, you may block such cookies using your browser. Some parts of our website may not work properly if you do.
 - d) 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. How and When Can You Withdraw Your Consent?

Much of what we do with your Personal Data is not based on your consent, instead it is based on other legal grounds. For processing that is based on your consent, you have the right to take back that consent for future processing at any time. You can do this by contacting us by email at service.malta@globalpay.com or calling our helpdesk on 2226 5656. The consequence might be that we cannot send you some marketing communications or that we cannot take into account special categories of Personal Data.

6. Is Your Personal Data Transferred Outside Malta or the EEA?

We are based in Malta, but we have other members of our Group outside Malta, and sometimes your Personal Data will be transferred outside Malta or the European Economic Area (EEA). If it is processed within Europe or other parts of the EEA, then it is protected by European data protection standards. Some countries outside the EEA do have adequate protection for Personal Data under laws that apply to us. We will make sure that suitable safeguards are in place before we transfer your Personal Data to countries outside the EEA that do not have adequate protection under laws that apply to us. As of the date of this Notice, your Personal Data will be transferred to: the United States, Canada, the Philippines, India. You should check our website, from time to time, where we will provide updates if we make changes to the countries to which your Personal Data is transferred.

For more information about suitable safeguards and (as 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.

7. How Do 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, access their website to seek any shared credit data and any other data that is available to the public from other sources such as the Law Courts, The Registry of Companies, VAT Department and other official sources that help us in our credit assessment.

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.

This information about CRAs is condensed. GPN will identify the CRA used in relation to your Personal Data on request, by emailing our Data Protection Officer as detailed above. You can contact the CRAs directly by visiting their websites to obtain a copy of your information from them.

- MACM - <https://www.macm.org.mt/>

8. How Do 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 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. GPN 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.

9. For How Long Is Your Personal Data Retained by Us?

Unless we explain otherwise to you, we will hold your Personal Data whilst you are receiving Services from us, and for a period of up to seven years afterwards, or such other longer period as may be required for regulatory compliance, in case you have any queries or any legal claim arises, and to comply with our own legal, regulatory and record keeping requirements.

10. What Are Your Rights under Data Protection Laws?

Here is a list of the rights that all individuals have under Data Protection Laws. They do not apply in all circumstances. If you wish to exercise any of them, we will explain at that time if they are applicable or not.

- 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;
- 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 the Commissioner of Information and Data Protection who enforces 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.

11. 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 **January 2024** and may be amended from time to time. Updated versions will be posted on our website as detailed above. We will notify you of changes to this document.

*Lines are open between 08:00 and 16:00 hours Monday to Friday, excluding public holidays. To help us continuously improve on our services and in the interests of security, we may monitor and / or record your telephone calls with us. Any recordings remain our sole property.

Global Payments Limited is a limited liability company registered in Malta number C54740.
Registered Office: Ground Floor, Continental Business Centre, Old Railway Track, Santa Venera, SVR9018, Malta.
Regulated by the Malta Financial Services Authority. (Ref No. 103028-08/18)