Title: Privacy Policy | Version: 3 | Updated: 09/09/2024 | Region: United Kingdom (GB)

This policy sets out the basis on which Guavapay Limited (Salisbury House, 29 Finsbury Circus, London, EC2M 5QQ, United Kingdom) (Company Number 10601900) (together with our subsidiaries, our holding company, subsidiaries of our holding company from time to time, collectively called "Guavapay", "MyGuava" or "we") collects personal data from you and how we process such data. By visiting our website www.guavapay.com or www.myguava.com (our "Website(s)"), you accept and consent to the practices set out below. If you have further questions, please get in touch with us by emailing us at support@guavapay.com or by chatting to us from MyGuava app.

1. Who's your controller?

Guavapay is the "Data Controller" of your personal information that is processed in connection with this Privacy Policy. Guavapay encompasses a range of companies who provide payments solutions and related services to individuals and legal entities. For the purposes of the applicable data protections laws, Guavapay is the data controller of your personal data unless otherwise specified. The Guavapay entity responsible for your data may depend on your location and the service you use with us.

2. The data we collect about you

We collect information about you in three ways: (i) when you provide it to us directly, (ii) when we gather information while you are using our services, and (iii) when we collect information from other sources. Please note that the personal data we collect, and process depend on the Service you use.

Below is a description of the types of information that we may receive directly from you.

"Identity Data" includes first name, last name, username, identification number, email address, address and telephone numbers.

"Call Recording Data" includes information collected when recording telephone calls which you make to us or receive from us.

"Financial Data" includes without limitation (i) bank account details such as Bank Identification Number (BIN), international bank account number (IBAN) or virtual international bank account number (VIBAN); and (ii) card details such as card type, card number, postcode, expiry date, country of issue, CAV2/CVC2/CVV2/CID, PIN and the last four digits of the card number (often such information is collected for authorisation purposes and not stored).

"Job Application Data" includes your contact information (including name, postal address, email address and phone number), job history, curriculum vitae, contact details of your referees and any other personal information you choose to submit along with your application when applying for a job at Guavapay or any of its affiliate entities. For further information please see our recruitment privacy notice.

"Other Information" you choose to provide. You may choose to provide other information, such as different types of content (e.g., photographs, articles, comments), content you make available through our live web chat function or through social media accounts or memberships with third parties, or any other information you want to share with us. We also get data from the devices you use when you interact with our systems, like your location or information about the device you're using.

"Technical Data" includes information we obtain from your device or browser (such as IP address, your login data, version and device identifiers, time zone setting and location (where permitted), browser plug-in types and versions and operating system) as well as how you use our website. We may automatically collect Technical and Usage Data about your equipment, browsing actions and patterns. We collect this personal data by using server logs and other similar technologies. We may also receive data about you if you visit other websites employing our cookies. We collect passwords and login date that you use on our Website and application. We collect details of authentication of device for purposes of Strong Customer Authentication such as SMS OTP and TOTP. Exceptionally we collect TAN and other security elements, including biometric elements such as Face-identification for payment authorisation and authentication.

"Commercial Data" includes information about the products and services you sell e.g., inventory, pricing and other data and information about your payment transactions e.g., when and where the transactions occur, a description of the transactions, the payment or transfer amounts, billing and shipping information, and payment methods used to complete the transactions.

We also need to check that you are eligible for the services you want to use, to assess your identity ("know your customer") and confirm that you are allowed to use our services legally ("due diligence"), and to protect your data and our services from potentially fraudulent activities which may put you and your money at risk. To do this, we may collect data about you from companies that help us verify your identity, do a credit check, prevent fraud or assess risk, which we refer to as "External Data".

"Background Data" includes Identity Data from publicly availably sources such as the company registrar and the electoral register in your country, as well as data from search information providers and third-party websites such as UK Companies House, search

engines and other public information sources.

“Due Diligence Data” includes any such information that we may need to comply with anti-money laundering or similar legislation, such as identification documents (identity cards, passports or equivalent), pictures of yourself or other information that we may be required to collect to verify your identity.

“Fraud Data” account or credit-related information with any credit reporting agency or credit bureau.

In certain instances we also obtain information about your customers on your behalf as your service provider when they transact with you or otherwise when you request that we do so. We call this information “Customer Data”. We process Customer Data when they interact with you through your use of the Services, for instance when they make a payment at your establishment, or schedule an appointment, or receive an invoice from you. The particular Customer Data we collect will vary depending on your location, which Services you use and how you use them. Your Customers’ Data may include:

“Customer Device Data” includes information about your customer's device, including hardware model, operating system and version, device name, unique device identifier, mobile network information, and information about the device's interaction with our Services.

“Customer Financial Data” includes bank account and payment card numbers.

“Customer Identification Data” includes first name and last name.

“Customer Transaction and Refund Data” When your customers use our Services to make or record payments to you, we collect information about when and where the transactions occur, the names of the transacting parties, a description of the transactions which may include item-level data, the payment or transfer amounts, billing and shipping information, and the devices and payment methods used to complete the transactions.

We use Customer Data as part of our contractual obligation to provide the Services you request to you.

It is your responsibility to obtain any necessary permission for us to process Customer Data in the manner envisaged in this Policy so that we can provide you with the services requested by you.

3. Lawful basis for processing your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- where you've agreed to us collecting your personal data, or sensitive personal data, for example when you tick a box to indicate you’re happy for us to use your personal data in a certain way;
- for the performance of a contract, we are about to enter into or have entered into with you;
- in some cases, we have a legal responsibility to collect and store your personal data (for example, under anti-money laundering laws and financial reporting obligations we must hold certain information about our customers;
- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. We consider and try to balance the possible potential effects (positive or negative) and your rights before processing your personal data for our legitimate interests; and
- where we process your personal data, or your sensitive personal data (sometimes known as special category personal data), to adhere to government regulations or guidance, such as our obligation to prevent fraud or support you if you are or become a vulnerable customer.

You have the right to withdraw consent at any time.

4. Purposes for which we will use your personal data

We have set out below, a description of all the purposes for which we will process your personal data.

- If you are a legal entity, to register you as a new customer.

- If you are using our Services (either as our customer or a customer of our customer), to facilitate a transaction or to help you track settlements and monitor transactions in real-time.

- If you are a legal entity, to manage our arrangement with you, including: (a) managing payments, fees and charges; (b) collecting and recovering money owed to us.

- To provide the live chat function on our website to answer any enquiries from users regarding our services.

- If you opt to submit personal data to engage in an offer, program, or promotion, we use the personal data you provide to manage the offer, program, or promotion.

- To administer and protect our business (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).

- To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you.

- To use data analytics to improve our website, our services, marketing, customer relationships and experiences.

- To make suggestions and recommendations to you about our services that may be of interest to you.

- To comply with laws and to respond to and comply with requests from the government, regulators and other third parties with legal authority, including but not limited to: anti-money laundering, fraud, anti-terrorism, anti-slavery or similar legislations.

- To investigate, detect and prevent fraud or crime.

- To exercise or defend legal claims.

- To consider your application for a job.

We will only process your personal data for the purposes specified above unless we reasonably consider that we need to use it for another reason which is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and explain to you the legal basis which allows us to do so.

Our services are not directed to people under the age of 18 (eighteen), and we request that they do not provide personal data to seek services directly from Guavapay. In certain countries, we may impose higher age limits as required by applicable law.

5. Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We may use your Identity Data and Technical Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which Services and offers may be relevant for you (“Marketing and Communications Data”).

You would receive marketing communications if you purchased similar goods or services or have been in contact with us about similar goods or services. We would also send you marketing communications when you have given your consent for us to do so.

We also may contact you where we have obtained your details from ‘B2B’ business data and marketing solutions providers.

You can ask us to stop sending you marketing messages by contacting us at any time at support@guavapay.com or chat to us from MyGuava app.

6. Disclosures of your personal data

We may share the personal information described in section 2 for the purposes set out in section 4 with the following service providers and third parties:

- Service providers who provide IT and system administration services.
- Credit card networks and payment networks such as Visa and Mastercard.
- Professional advisers who legitimately need to have access to the personal data for a business need.
- Fraud prevention agencies (see more on that below), regulators and other authorities who require reporting of processing activities in certain circumstances.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Policy.
- Your personal information may be shared with the companies within our group. We share information with them, so they can assist us in providing services to you and to understand more about you.

All Guavapay group companies have a legitimate business interest (i.e., to provide a complementary or related service for your business) in accessing the data and may do so for the purposes and in the way described in this Policy. Guavapay group companies shall be taken to include any entity that directly or indirectly controls, is controlled by, or is under common control with from time to time, whether located in or outside of the United Kingdom. When we transmit data between our group entities located inside and outside of the EEA, this sharing is governed by our intra-group data sharing and processing agreement which is drafted in compliance with the GDPR and includes the relevant safeguards necessary for transfers outside the EEA.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and, unless otherwise notified to you, only permit them to process your personal data for specified purposes and in accordance with our instructions.

Fraud prevention agencies: The personal information we have collected from you will be shared with fraud prevention agencies, including but without limitation, CIFAS (https://www.cifas.org.uk/), who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance, or employment. Further details of how your information will be used by CIFAS, and your data protection rights (in addition to those set out in this Policy), can be found by visiting www.cifas.org.uk/fpn.

7. International transfers

Many of our external third parties are based outside the EEA or the UK so their processing of your personal data will involve a transfer of data outside the EEA or the UK.

Whenever we transfer your personal data out of the EEA, we will take reasonable steps to ensure that your personal data is kept secure, including where relevant, by entering into appropriate contractual terms with the receiving party outside the UK or EEA, such as the Standard Contractual Clauses approved by the EU Commission or issued by the UK Information Commissioner's Office (as applicable) or any other approved mechanisms that may become available to us in the future. We will also carry out a risk assessment of the laws and practices of the destination country to identify any technical and organisational measures that need to be put in place to ensure that your personal information is fully protected when transferred to that country.

8. Data security

Data security is extremely important to us, and we have put in place appropriate security measures (such as encryption, confidentiality obligations of our personnel, log-in records, vulnerability testing etc,) to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know.

We have put in place procedures and incident management policies to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

9. How long we retain your information

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including the purpose of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the relevant laws, amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we

process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes.

Even after we stop providing services directly to you, we may continue to retain your personal data to: (1) comply with our legal and regulatory obligations; (2) enable fraud monitoring, detection, and prevention activities; and (3) comply with our tax, accounting and financial reporting obligations.

The table below outlines different categories of personal data collected, along with the retention period or the criteria used to determine that period.

CATEGORIES OF PERSONAL DATA COLLECTED	RETENTION PERIOD OR THE CRITERIA USED TO DETERMINE THAT PERIOD
Identity Data Call Recording Data Financial Data Fraud Data	For the duration necessary for Guavapay to: (1) comply with law provide the services; and (3) pursue the legitimate interests, incl detecting and preventing fraud and financial crimes, enforcing a defending our legal rights, complying with valid legal process re from courts or competent authorities, improving the quality of o services, and promoting our products and services as appropriate as permitted by applicable law and agreements.
Due Diligence Data	No longer than 1 year, or upon revocation of your consent, whic is earlier.
Technical Data Commercial Data Background Data	For the duration necessary for to: (1) comply with law; (2) provi services, and; (3) pursue our legitimate interests, including detec and preventing fraud and financial crimes, enforcing and defend legal rights, and complying with valid legal process requests fro courts or competent authorities.
Job Application Data	For the duration necessary to: (1) comply with law; (2) make cer employment and performance-related decisions; (3) address futu hiring needs; (4) ensure health and safety in the workplace; (5) c certain administrative tasks, including to administer benefits; an pursue our legitimate interests, including enforcing and defendi legal rights and complying with valid legal process requests fro courts or competent authorities.

10. Automated decision making

We may sometimes use systems to make automated decisions about you or your business to provide you with a better and safer experience. We may use information that we already have or that we can collect from third parties. We may use automated decision making to:

- Approve or deny your applications for some of our services or products.
- Determine pricing and rates for some of our services, for example access to credit.
- Provide you with tailored offers.
- Detect fraud and comply with anti-money laundering legislation.

You can object to automated decision making and ask that a person reviews it.

11. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your Personal Data. You have the right to:

- Request access to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected.
- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it.
- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party).
- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data’s accuracy; (b) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (c) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Request the transfer of your personal data to a third party. We will provide to the third party you have chosen, your personal data in a structured, commonly used, machine-readable format.
- Withdraw consent at any time where we are relying on consent to process your Personal Data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
- Right for you not to be subject to a decision based solely on an automated process, including profiling, which produces legal effects concerning you or similarly significantly affect you.

If you wish to exercise any of the rights set out above, please email DPO@guavapay.com.

No fee is usually required to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you is specific information to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights).

Time limit to respond, in cases of legitimate requests, is one month. Occasionally it may take us longer than one month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

12. Where we store your personal data

Our operations are supported by a network of computers, servers, other infrastructure and information technology, and third-party service providers. We and our third-party service providers and business partners store and process your personal data in the European Union, the United Kingdom. Courts, law enforcement and security agencies of these jurisdictions may be able to use legal processes to access your personal data.

13. Changes to this Policy and yocomplaur duty to inform us of changes

Guavapay reserves the right to change, modify or amend this Policy at any time, but will not reduce the level of privacy protection contained herein.

14. Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

Please refer also to our Cookie Policy which explains the use of cookies on our websites and applications.

15. Contact

If you have questions or concerns about this Privacy Policy, or would like to , feel free to contact our Customer Support 24 hours a day, 7 days a week, as follows:

- You can write to us at the address: Customer Support, Guavapay Limited, Salisbury House, 29 Finsbury Circus, London EC2M 5QQ, United Kingdom.

- You can chat with us through the app or website.

- You can email us at DPO@guavapay.com.

- You can call the Customer Support on +44 204 577 1440.

16. Complaints

Please If you have any concerns about our use of your personal information, you can make a complaint to us at DPO@guavapay.com. Please also see the Complaints section on our Website.

You can also complain to the relevant Data Protection Authority if you are unhappy with how we have used your data. In the United Kingdom this would be the Information Commissioner’s Office, you may wish to follow the link on the ICO’s website at https://ico.org.uk/make-a-complaint/ in order to submit a complaint.