INFORMATION SECURITY

DATA PRIVACY & SECURITY STATEMENT

Table of Contents

INFORMATION SECURITY 1
1. Objective 3
2. Scope 3
3. Responsibilities 3
4. Background 3
5. Data Security Statement 3
International Data Transfers 4
Technical and organizational security measures 4
6. Revision History 6

1. Objective

The purpose of this document is to establish LocalPayment's Data Privacy & Security Statements.

2. Scope

LocalPayment establishes the privacy and security compliance commitment, and the technical and organizational security measures needed to safeguard the customer's information.

3. Responsibilities

Information Security, Compliance and Legal departments must review this statement at least annually and carry out the actions needed to keep this statement updated as LocalPayment Security and Privacy evolves over time, or when required for any regulation or by law.

4. Background

As the regional leader in Payment processing for international companies, with a strong presence in the Latam market, LocalPayment has a strong commitment to safeguard its customers' information and make them feel and know their information is properly secured.

This Data Privacy & Security Statement seeks to clarify LocalPayment efforts to comply with personal data regulations.

5. Data Security Statement

LocalPayment strongly believes that information security and privacy are fundamental principles for all Company activities. In line with these principles, LocalPayment has put in place a robust security and privacy program embracing data protection across the Company.

The General Data Protection Regulation (GDPR) is a comprehensive new privacy law that gives residents of the European Union (EU) greater control over their "personal data" and requires organizations to maintain appropriate security while processing it.

LocalPayment as a data processor:

- Will only act on written instructions of the controller (i.e. customer, set out in a Data Processing Agreement)
- Keep records of the processing activities.
- Engage subprocessors (i.e. contractors) only with prior written authorization of the controller.
- Ensure the security of its processing by implementing appropriate technical and organizational measures.
- Notify any Personal Data breaches to the controller without undue delay after becoming aware and to the data protection authorities within 72 hours.
- Provide adequate safeguards to transfer Personal Data to a country outside the European Economic Area (EEA) ("Third country").

- Ensure that persons authorized to process Personal Data have committed themselves to data secrecy/confidentiality agreements.
- Inform the controller if LocalPayment receives a request from a data protection authority or individuals to exercise data subject's rights.
- Upon controller's instruction delete or return all the Personal Data after the end of the provision of services.
- Make available to the controller all information necessary to demonstrate compliance and cooperate in audits.

If LocalPayment is required by a governmental authority or by order of a court of competent jurisdiction to disclose any of controller's confidential information, LocalPayment will give controller prompt written notice thereof and LocalPayment will take all reasonable and lawful actions to avoid or minimize the degree of such disclosure. LocalPayment will cooperate reasonably with controller in any efforts to seek a protective order.

International Data Transfers

Pursuant to GDPR, when a controller or processor wishes to transfer personal data to a Third Country, the third country must ensure that it has an adequate level of protection for the personal data as determined by the European Commission ("Commission") or provide appropriate safeguards on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

LocalPayment currently uses the Standard Contractual Clauses as a mechanism to legitimize international data transfers to countries that are not deemed to provide an adequate level of protection and has deployed a mechanism that provides appropriate safeguards for the data. Therefore, third country transfer will be based on Standard Contractual Clauses and incorporated in the form of a Data Processing Agreement ("DPA") between LocalPayment and its customers. LocalPayment will not transfer personal data that processes on Customer's behalf to any third country, unless and according to the Commission, a mechanism that provides appropriate safeguards for data is properly deployed.

Technical and organizational security measures

LocalPayment has implemented the following categories of technical and organizational security measures to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to customer personal data.

- Defining, publishing and communicating to staff and sub-processors a set of policies for information security.
- Maintaining an Information Security awareness and training program to all Company staff.
- Reviewing policies for information security on planned intervals or when significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
- Performing pre-hire screening and background checks consistent with local hiring practices and laws.

- Holding staff with access to personal data accountable for maintaining confidentiality obligations.
- Requiring business ethics, data security, and international data privacy training upon initial hire and at least annually.
- Making copies of security standards and procedures available to all staff.
- Establishing an appropriate access control policy and reviewing it based on business requirements and related information security requirements.
- Assigning responsibility for information security practices and standards as part of an information security program.
- Granting the minimum necessary logical access to support the data processing services.
- Removing access for terminated staff promptly.
- Requiring regular password changes for staff with access to personal data.
- Requiring secure log-on procedures to access to personal data.
- Controlling changes to Information Systems that affect personal data.
- Monitoring the capacity and availability of information resources that store, process or transmit personal data.
- Protecting facilities against reasonable physical and environmental threats such as natural disasters, fires, etc.
- Destroying physical media using industry standard practices; encrypting backups if using removable tape or other media.
- Providing network protections like firewalls, intrusion detection and monitoring for unauthorized access.
- Securing personal data transmitted over the internet and between external networks with industry standard encryption.
- Periodically conducting vulnerability tests; regularly applying security patches; implementing malware protection for servers and workstations.
- Periodically checks on company internal policies.

Privacy Policy

Introduction

LocalPayment ("LocalPayment", "we" or "us") respects your privacy and is committed to protecting it through our compliance with this Privacy Policy ("Policy"). This Policy explains what personal data LocalPayment collects on customers, partners, vendors and marketing contacts, and how we use it. By accessing or using the website, you agree to the policies and practices described in this Policy. LocalPayment may change this Policy from time to time. Your use of the website at any time indicates your acceptance of the version of this Policy posted on the website at such time, so please check this Policy periodically for updates.

What personal data does LocalPayment have?

We may collect and process your name, email address, job information, phone number, address and cookie information. Personal data can be collected when voluntarily submitted or provided by you through sales enquiries, marketing events, downloads, use of LocalPayment platform, customer portal and website ("Website") and from third parties.

The information we collect on or through the Website may include information you provide by filling in forms or making other affirmative choices on the Website, details of transactions you carry out through the Website and information we collect through automatic data collection technologies ("Cookies"). As you navigate through and interact with the Website, we may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, including (i) details of your visits to the Website, such as traffic data, logs, navigation data and other communication data and the resources that you access and use on Website; and (ii) information about your computer and internet connection, including your IP address, operating system, and browser type.

The information we collect automatically is statistical data and may include personal data, but we may maintain it or associate it with personal data we collect in other ways or receive from third parties. This information helps us to understand our user base and usage patterns, store information about your preferences, allowing us to customize our Website, improve the Website and deliver better service; and recognize you when you return to the Website.

The technologies we use for automatic data collection may include:

- **Browser cookies**

  A browser cookie is a small file placed on the storage unit of your device. A cookie file can contain data such as a user ID that the site uses to identify your computer or device

and to identify the pages you've visited, but the only personal data a cookie can contain is data you supply yourself. Your browser is most likely set to accept cookies. However, if you would prefer not to receive cookies, you can alter the configuration of your browser to refuse cookies. If you choose to have your browser refuse cookies, it is possible that some areas of our Website will not function properly when you view them. Note that third parties collect and use data from Cookies placed on the Website. This Privacy Policy may not describe the privacy practices of such third parties. We encourage you to read the privacy policies of these third parties and, if you prefer to not have data reported by these parties, follow their opt-out processes where these exist.

- **Web beacons**

  Pages of the Website may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit us to ascertain the effectiveness of our product, service campaigns and marketing programs; allow us to customize the services offered on or through our Website; and help us determine the best use for Website content, and product and service offerings.

External or Third-Party Websites

To the extent hyperlinks are utilized to access external or third-party sites, you should be aware that these external or third-party sites are not controlled by LocalPayment and, therefore, are not subject to this Policy. LocalPayment suggests that you check the privacy policies of these sites to determine how your personal data will be utilized by the proprietors of those third-party sites.

How is my personal data used?

If you are a customer or a partner your personal data will be used for contract management, sales administration, LocalPayment customer portal access and product updates. This will allow us to fulfil our contractual obligations owed to you and to support our business relationship with you. We will also use your personal data to verify your identity, communicate with you, arrange the delivery or other provision of products and services, provide customer services and respond to your product support requests.

If you provide us with your personal data using one of our Website forms, we will hold this information to track if you visit the LocalPayment Website again, and to follow up with you if you request LocalPayment to do so. We may also collect information about the use of the LocalPayment Website such as the types of information accessed and how many users, we receive daily. LocalPayment may use this data to help us monitor, improve and protect our products, content, services and for statistical analysis, marketing, or similar promotional purposes.

We may also use your personal data for marketing purposes if we have your consent or a legitimate interest in doing so. We may, from time to time, contact you to keep you informed about our products and services, special offers, events or our selected partners' products and services. You can unsubscribe from marketing emails at any time.

On other occasions, we may also use your personal data for any other purpose with your consent and we will use the data for the purpose which we will explain at that time.

Is my personal data shared with third parties?

We may share your personal data with other LocalPayment companies. Where another LocalPayment company processes your information the same principles of this Policy will apply. We may also share your personal data with our suppliers to process your personal data on our behalf. If you would like further information on our suppliers and their privacy policies, please contact us at legal@LocalPayment.com

If LocalPayment needs to transfer your personal data to a third party outside of the European Economic Area we will ensure that your personal data is appropriately protected through EU US Privacy Shield, standard contractual clauses approved by the EU Commission or other means approved by our supervisory authority.

We may disclose your personal data that we collect, or you provide as described in this Policy:

- to fulfill the purpose for which you provide it;
- to support our business (such as helping to provide our Services, for promotional and/or marketing purposes, and to provide you with information relevant to you such as product announcements, software updates, special offers, or other information) and who are bound by contractual obligations to keep personal information confidential and use it only for the purposes for which we disclose it to them;
- to analytics providers such as Google Analytics. Google Analytics uses cookies to collect non-identifying information. Google provides some additional privacy options regarding its Analytics cookies at http://www.google.com/policies/privacy/partners/.
- for any other purpose disclosed by us when you provide the information;
- for any other purpose with your consent;

We may also disclose your personal data as is necessary to: (a) comply with a subpoena or court order; (b) cooperate with law enforcement or other government agency; (c) establish or exercise our legal rights; (d) protect the property or safety of our company and employees, contractors, vendors, and suppliers; (e) defend against legal claims; (f) help with internal and external investigations; or (g) as otherwise required by law or permitted by law or if required for the legal protection of our legitimate interests in compliance with applicable laws.

In the event that our business is sold or integrated with another business, your data will be disclosed to our advisers and any prospective purchaser's adviser and will be passed to the new owners of the business (subject to the applicable laws).

What rights do I have on the data you have about me?

You have the right to request a copy of the personal data LocalPayment holds about you and to have any inaccuracies corrected. You also have the right to have your personal data removed from our marketing database if you no longer wish to receive marketing communications. Please send your requests to legal@LocalPayment.com

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, where they would infringe the rights of a third party (including our rights) or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping. Relevant exemptions are included in the GDPR. We will inform you of relevant exemptions we rely upon when responding to any request you make.

How long will you keep my personal data?

For customers, partners and vendors, we will keep your personal data for up to six years after your contract with us ends or for as long as required pursuant to applicable legal and/or regulatory requirements.

For portal users, we will keep your personal data for as long as you are an active user of our Website and for up to five years after this. For marketing contacts, we will keep your personal data until your request us to stop and for a short period after this (to allow us to implement your request). We will also keep a record of the fact that you have asked us not to send you direct marketing or to process your data indefinitely so that we can respect your request in future.

How do I complain about use of my personal data?

If you would like to make a complaint about our use of your personal data please send details of your complaint, including the personal data it relates to, to legal@LocalPayment.com. We will investigate your complaint and respond as soon as we can, and no more than one month later. If you have unresolved concerns, you have the right to complain to an EU data protection authority where you live, work or where you believe a breach may have occurred.

General Data Protection Regulation ("GDPR")

Data and its protection are becoming increasingly important to individuals and enterprises. On May 25, 2018, the European Union has enacted the most significant pieces of legislation intended to protect personal data, the General Data Protection Regulation ("GDPR"). The GDPR is designed to establish one set of data protection rules across the European Economic Area ("EEA"). The GDPR applies to organizations that process EEA personal data, even if that organization is established outside of the EEA.

The terms "Data Controller", "Data Processor", "Personal Data", "Processing" and "Subprocessor" shall have the same meaning as defined in the Standard Contractual Clauses and Article 4 GDPR;

Pursuant to Article 28 of the GDPR, LocalPayment has certain obligations as Data Processor relating to its processing of personal data and expressly commits to:

- Only act on written instructions of the Data Controller (i.e. customer set out in a Data Processing Agreement).
- Implement technical and organizational measures to ensure the adequate protection of Customer's Personal Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32.
- Notify Data Controller, without undue delay, if LocalPayment becomes aware of breaches of the protection of personal data and to the data protection authorities within 72 hours.
- Engage Subprocessors (i.e. contractors) only with prior written authorization of the Data Controller.
- Ensure that persons authorized to process Personal Data have committed themselves to Data Secrecy/Confidentiality Agreements.
- Inform the Data Controller if LocalPayment receives a request from a data protection authority or individuals to exercise data subject's rights.
- Upon Data Controller's instruction correct, delete or return all the Personal Data after the end of the provision of services.
- Make available to the Data Controller all information necessary to demonstrate compliance and cooperate in audits.

International Data Transfers

Pursuant to GDPR, when a Data Controller or Data Processor wishes to transfer personal data to a Third Country, the third country must ensure that it has an adequate level of protection for the personal data as determined by the European Commission ("Commission") or provide appropriate safeguards on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

LocalPayment uses the Standard Contractual Clauses as a mechanism to legitimize international data transfers to countries that are not deemed to provide an adequate level of protection and

has deployed a mechanism that provides appropriate safeguards for the data. Therefore, third country transfer will be based on Standard Contractual Clauses and incorporated in the form of a Data Processing Agreement ("DPA") between LocalPayment and its customers. LocalPayment will not transfer personal data that processes on Customer's behalf to any third country, unless and according to the Commission, a mechanism that provides appropriate safeguards for data is properly deployed.

Children Under the Age of 16

LocalPayment will not collect personal data from any person who is actually known to us to be under the age of 16. If we become aware that a person under 16 has provided personal Data, LocalPayment will take steps to remove such data and terminate that individual's account, access and use of the Website. If you believe we might have any information about a child under 16, please contact us at legal@LocalPayment.com

State of California Residents

Under California Civil Code Section 1798.83 (the "Shine the Light" law), California residents who provide personal information in obtaining products or services from LocalPayment are entitled to request and obtain from us once a calendar year information about the customer information we shared, if any, with other businesses for their own direct marketing uses. If applicable, this information would include the categories of customer information and the names and addresses of those businesses with which we shared customer information for the immediately prior calendar year (e.g., requests made in 2016 will receive information regarding 2015 sharing activities). If you are a California resident and would like a copy of this information, please submit a written request to: legal@LocalPayment.com

Contact

We hope that we can satisfy any queries you may have about the way we process your data. If you have any concerns about how we process your data, or would like to opt out of direct marketing, you can get in touch at legal@LocalPayment.com