Worldpay Privacy Notice

Introduction

Worldpay, LLC, a subsidiary of Fidelity National Information Services Inc, ("**FIS**"), and its subsidiaries and related entities, collectively known as Worldpay from FIS ("**Worldpay**" or "**we**" or "**our**"), recognizes and respects the privacy of individuals whose personal information it collects, uses and stores in the course of conducting business. We are committed to processing personal information in accordance with applicable privacy laws and regulations, including the General Data Protection Regulation ("**GDPR**"), as described in this Privacy Notice. Where we refer to personal information, this includes "personal data" as defined in the GDPR and other applicable privacy laws in countries and territories where Worldpay operates.

This Privacy Notice explains to individuals who access or use Worldpay's services, including those who interact with our websites, mobile sites, and applications ("**Sites and Services**") ("**you**"), how Worldpay uses your personal information. This includes buyers, Worldpay merchants and other Worldpay customers who trade as individuals, as well as website or app users. In some circumstances, you have the right to object to our processing of your personal data and you can ask us to restrict our use of your personal data and to erase it. Please see under the "Choices and Rights" section for more information.

When Worldpay uses the word "buyer" in this Privacy Notice, this means any shopper or individual whose payment transactions may be processed using Worldpay's Sites and Services.

This Privacy Notice is global in scope but is not intended to override any legal rights in any territory where such rights prevail.

The Worldpay entity responsible for collecting, storing or using your personal information (that is, the "controller" where the GDPR or the United Kingdom Data Protection Act 2018 apply) depends on why or how you interact with Worldpay and location. If you have any questions about which entity this is, please contact us through the details set out in the "Contact Us" section below.

Personal information used by Worldpay

Worldpay collects personal information relating to buyers, merchants, or other customers, in order to carry out its business activities. Worldpay may collect personal information from various sources, including:

- information provided to us, either directly or via our merchants, or other customers;
- information automatically collected when you use our Sites and Services, including but not limited to our role as a payments processor;
- information collected by cookies and other tracking technologies when you use our Sites and Services – please see our Cookie Notices for more information about the cookies and other tracking technologies we use:
    - on FISglobal.com;
    - on Merchant Solutions; and
    - on Merchant Solutions (Denmark only); and
- information collected from third parties, including but not limited to: fraud monitoring service providers, commercial databases, or know your customer (**KYC**) service providers.

This personal information may include:

- **Contact information**, including but not limited to: name (first, last, and business), telephone numbers, address (home, billing, and business), fax, email address, and other communications;
- **Demographic information**, including but not limited to: nationality, country of residence, date of birth, marital status, birth place, gender, preferred language, citizenship;
- **National Identification information**, including but not limited to: national insurance number, passport, social security number, taxpayer identification number, driver license or other form of identification to verify a buyer, merchant or other customer;
- **Monitoring or Recording**, including but not limited to: monitoring or recording telephone calls, emails, web chats, CCTV, access control, or other communications;
- **Merchant or other Customer identification**, including but not limited to: merchant or customer ID;
- **Merchant or other Customer management,** including but not limited to: billing, invoicing, refunds, financial position (including debt position), reconciliations and reporting;
- **Information related to items purchased**, including but not limited to: location of the purchase, value, time, method, any feedback that is given in relation to such purchase;
- **Payment transaction information**, including but not limited to: which Alternative Payment Method ("**APMs**") is used (e.g. bank transfer, pre-pay service, post-pay service, eWallets and local card schemes), transaction monitoring and fraud monitoring information (e.g. transaction values and volumes, risk scores attributed to transactions, merchant category code, IP address from where a transaction is made (optional), buyer email address (optional)), and analytics or trend analyses related to a customer's sales or refunds (including chargebacks);
- **Financial and credit/debit card information**, including but not limited to: payment account number (PAN) or account number, card expiration date, CVC details, bank and/or issuer details;
- **Credit, fraud, sanctions and transaction risk information**, including but not limited to: information obtained about our customers from credit reference or fraud prevention agencies, including credit history, credit score, and business name, business address and any business ID (such as the registered number or VAT number), financial statements for the applicant or companies within the same group of companies of the applicantand payment transaction information from our fraud and transaction monitoring activities which relates to our customers, such as transaction types, values and risk scores;
- **Technical information**, including: the IP address used to connect your computer or device to the Internet, your device ID, login information (username/password), browser type and version, time zone setting, browser plug-in types and versions, device operating system platform, mobile carrier, location or GPS/geo-location;
- **Information about your visit or whether you opened an email**, including: the full Uniform Resource Locators (URL) clickstream to, through and from Worldpay's site (including date and time), products or services you viewed or searched for page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks and mouse-overs), methods used to browse away from the site page, any phone number used to call Worldpay's customer service number;
- **Photographs and videos of you,** from Worldpay events, e.g. through identity verification;

- **Publicly accessible comments and opinions** reviewed and used by Worldpay, through Internet searches or posted on social networking sites, such as Facebook and LinkedIn;
- **Insights** gained through Worldpay gatherings from sessions that you participate in and contribute at Worldpay events;
- **Social media posts** on Worldpay social media sites or made publicly about Worldpay on social media**;**
- **Event participant details** from a Worldpay event, including but not limited to: name, title, and company from a Worldpay app for the event which is available to registered delegates; and
- **Applications**, if you download or use mobile or desktop applications, including information about your location, your device or the service you are using, including where a payment transaction takes place.

For more detailed information on the purposes of processing, and the legal basis on which Worldpay relies to process, please consult the Appendix to this Notice.

Worldpay's sharing of personal information

Worldpay may make personal information available to:

- other parts of Worldpay, or FIS group companies;
- third-party service providers, including information technology service providers (e.g. for cloud computing), risk, fraud, and compliance service providers (e.g. for transaction risk monitoring); debt service providers (e.g. for debt collection analysis or management); and for business analytics (e.g. for data aggregation, visualisation and reporting);
- our business partners, including payment processors, payment infrastructure providers, digital wallet providers, banks and other financial institutions;
- advertisers (where a Worldpay customer opts-in to this service);
- our professional legal advisors (accountants, consultants, lawyers and tax advisors);
- law enforcement, regulatory, prosecuting, tax or governmental authorities, courts or other tribunals or dispute resolution bodies;
- prospective sellers or buyers as part of a sale or merger of our company, business or assets; and
- any other third party to the extent the disclosure is required by a law which applies to us.

As Worldpay is a global business, the above recipients may be based internationally (that is in a different country or territory to you), and some will be based outside of the European Economic Area or United Kingdom.

International transfers of personal information

In the ordinary course of global business operations, Worldpay transfers personal information across borders to its various branches and offices, or to third parties as set out above including, but not limited to, third-party service providers.

Where the GDPR or the United Kingdom Data Protection Act 2018 apply, if we transfer personal information to a recipient based in a jurisdiction outside of the United Kingdom or European Economic Area which is not subject to a European Commission adequacy decision (in other words, official approval for us to transfer personal information to those recipients), or equivalent, we will where feasible put in place European Commission-approved standard contractual clauses (or equivalent) to protect this personal information. We might also rely on other permitted transfer mechanisms such as relying on a relevant third party's "binding corporate rules" (approved by United Kingdom or European Union data protection authorities and put in place to protect your personal information). We may rely on other transfer mechanisms or legal bases available to us.

In relation to FIS Worldpay South Africa (Pty) Ltd, if we transfer personal information to a recipient based in a jurisdiction outside the Republic of South Africa, we will ensure that we comply with the provisions of POPIA.

We might, for example, rely on permitted transfer mechanisms such as transborder transfer agreement(s), "binding corporate rules" or other transfer mechanism(s), where applicable.

Retention

Worldpay will retain personal information only for as long as it is needed for the purposes for which we use it, in accordance with our retention policy. You may request further details about how long we hold your personal information by contacting us as set out in the "Contact Us" section below.

Security

Worldpay is committed to the confidentiality and security of personal information. Worldpay's systems and facilities in which personal information are processed are protected by secure network architectures that contain firewalls and intrusion detection devices.

Choices and Rights

Individuals may request further details regarding Worldpay's use of personal information in accordance with local applicable law.

Under the GDPR and United Kingdom's Data Protection Act 2018 and certain other applicable data protection laws, individuals are entitled:

- to ask for a copy of their personal information;
- to request that we correct or update inaccurate or incomplete personal information;
- in certain circumstances, to require us to erase their personal information or transfer it to another organisation, or to restrict (i.e. temporarily or permanently stop) all or some of our use of their personal information;
- to object to personal information being processed for direct marketing purposes;
- to request more information about our legitimate interests balancing test, where this is our lawful basis;
- where applicable, to object to our use of their personal information when this is based on our or a third party's legitimate interests;
- where applicable, to withdraw consent where we have asked for it to process personal information;
- where applicable, to not be subject to a decision based solely on automated decision making, including profiling, where the decision would have a legal effect on an individual or produce a similarly significant effect; and
- to ask us for a copy of the safeguard we use for a transfer of their personal data to a recipient based outside of the United Kingdom or European Economic Area.

These rights may be limited, for example, if fulfilling a request would reveal another person's personal information, or if the processing is required by law or other compelling legitimate interest.

To exercise their choices or rights, individuals should contact the FIS Privacy Office.

Complaints (UK and EU)Under the GDPR and United Kingdom's Data Protection Act 2018, individuals have the right to complain to a data protection authority in the United Kingdom or the European Union Member State where they reside, where they work or where the alleged infringement of data protection law occurred.

Links to third party sites

Our Sites and Services may, from time to time, contain links to and from the websites or services of merchants, partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites or services may have their own privacy policies and we do not accept any responsibility or liability for these policies, nor do we endorse such websites or services. We advise that you check any relevant terms before you submit any personal information to these third parties.

PERSONAL DATA PROTECTION IN ARGENTINA

The owner of the personal data has the right to access to such data free of charge at intervals of not less than six months. Such six month term may be shorter in case a legitimate interest is evidenced to that effect, as provided in paragraph 3 of article 14 of Law Nbr. 25,536.

The Agency for Public Information Access ("**Agencia de Acceso a la Información Pública**"), which is the competent authority under Law 25,326, has the power to deal with complaints and claims that are filed in relation to non-compliance with the personal data protection requirements.

The contact information of the "Agencia de Acceso a la Información Pública" is the following:

Address: Av. Pte. Gral. Julio A. Roca 710, 3rd floor - Autonomous City of Buenos Aires

Postal code: C1067ABP

Email: info@aaip.gob.ar

PERSONAL DATA PROTECTION IN MALAYSIA

In accordance with the Personal Data Protection Act 2010 ("**PDPA**"), Worldpay may:

a. Charge an administration fee for processing a data subject's request for access to personal information; and

b. Refuse to comply with a data subject's request for access or correction of the personal information.

Worldpay shall take necessary measures as described in this Privacy Notice to safeguard any personal information transferred outside Malaysia to ensure compliance with the PDPA.

In the event of any inconsistency between the English version and any other translation of this Privacy Notice, the English version shall prevail.

PERSONAL DATA PROTECTION IN SOUTH AFRICA

In accordance with the South African Protection of Personal Information Act, 2013 ("**POPIA**"), FIS Worldpay South Africa (Pty) Ltd is the entity responsible for collecting, storing or using your personal information for the purposes of any merchant services offered out of South Africa. For any enquiries, please contact the South African data protection officer at catherine.gliksman@fisglobal.com

The Information Regulator is the competent authority under section 39 of POPIA to deal with complaints and claims that in relation to non-compliance with the personal information protection requirements under POPIA. The Information Regulator's contact details are available at https://www.justice.gov.za/inforeg/contact.html

Changes to this Notice

As this Notice is updated or modified, the current version will be posted–on the Worldpay Privacy section of fisglobal.com.

Contact Us

If you have any questions related to Worldpay's processing of your personal information, please send your inquiries to:

Chief Privacy Officer
FIS
601 Riverside Avenue
Jacksonville, FL 32204

privacyoffice@fisglobal.com

If you are based in the European Economic Area (EEA) or Switzerland, you may contact the Worldpay Data Protection Officer at the following address:

Data Protection Officer
FIS
25 Canada Square, Canary Wharf
London E14 5LQ
United Kingdom

data.protection@fisglobal.com

APPENDIX

Why Worldpay processes personal information

We collect, use and store your personal information for the reasons set out in the table below.

We may also use your personal information where this is not incompatible with the original purpose for which we obtained it, and for any other purpose that we specifically tell you about.

In some cases, where you are required to provide your personal information because of a legal or contractual duty, your failure to provide the information in these circumstances could result in us being unable to fulfil our relationship with you.

Purpose of processing		Legal ground(s) for use
Designing, evaluating, benchmarking, and administering:	Worldpay product and service offerings and their relevance for particular merchants, or customers.	Worldpay relies on: • Consent to send promotional material (if required); • Worldpay's legitimate interests in protecting and enforcing its rights or to send promotional material; • Worldpay's legitimate interests in developing and improving products and services; and • The need to process personal data in order to provide a requested product or service or to fulfil a contract.
	Diversity programs, including compliance with diversity objectives	
	Worldpay controlled recognition and rewards programs for our merchants or other customers	
	Education, training, and awareness programs for our merchants or other customers	
	Sales and marketing campaigns	
	Offers of products and services, and contracts	
	Accounts receivable, accounts payable, bad debt and reserves; bank accounts for payments and receipts	
Assembling, maintaining, and disseminating:	Customer-specific job assignments for sales, marketing, and collections	Worldpay relies on: • Worldpay's legitimate interests in the administration of its business or in meeting non-UK, EU or EU Member state internal record-keeping requirements; • Worldpay's legal obligations under UK, EU or EU Member State tax, audit or regulatory law to maintain internal records; and
	Customer directories	
	Emergency contact information for merchants or other customers	
	Identification credentials	
	Internal record-keeping and reporting, including reporting on credit and financial risk	

Purpose of processing		Legal ground(s) for use
	Providing reports and analytics to our merchants or other customers	• Worldpay's legitimate interests in assisting its merchants or other customers understand their transactions, or its contractual obligation to provide this information.
Supporting, monitoring, auditing, executing, and facilitating:	Business conferences and travel	Worldpay relies on: • Consent; • Worldpay's legitimate interests in the administration of its business; and • Worldpay's legitimate interests in protecting the integrity of Worldpay services, facilities and systems. • Worldpay's legitimate interests in preserving records for business purposes, assuring security at its facilities and systems, and making merchant or other customer contact information available to relevant employees; • Worldpay's legitimate interests in promoting, developing, and improving products and services; and • The need to process personal data in order to provide a requested product or service, or to fulfil a contract.
	Business negotiations and transactions (including due diligence)	
	Business operations, including customer billing	
	Business transition activities, including mergers, acquisitions, and divestitures	
	Company marketing efforts, including websites, conferences, brochures, and other promotional media events and materials	
	Compliance with contractual obligations; customer service and support or account management	
	Identification for security and systems/ facility authentication	
	Internal and external business communications and management reporting	
Complying with:	Applicable laws and regulations and industry requirements, including reporting and disclosure obligations.	Worldpay relies on: • Legal obligations to process personal information under UK, EU or EU Member State law; • Worldpay's legitimate interests to comply with non-UK, EU, or EU Member State laws and regulations, or industry (e.g. card scheme or Payment Card Industry) requirements; and • Worldpay's legitimate interests in protecting and enforcing its rights.
Conducting:	Audits and accounting, financial and economic analyses (including to assess financial and insurance risks)	Worldpay relies on: • Legal obligations under UK, EU or EU Member State audit, tax or regulatory laws. • Worldpay's legitimate interests in meeting non-UK, EU, or EU Member State audit, tax or regulatory requirements. • Worldpay's legitimate interests in analyzing performance, understanding Worldpay merchant or other customer preferences,;
	In accordance with local law, investigations into alleged policy or contractual violations by merchants or other customers	
	Opinion and engagement surveys	

Purpose of processing		Legal ground(s) for use
		• Worldpay's legitimate interests in protecting the integrity of Worldpay Sites and Services, operations, facilities and systems; and • Worldpay's legitimate interests in protecting its rights.
Protecting:	Security of Worldpay assets, by implementation of identity authentication and other security measures, control of access to Worldpay and customer workplaces and systems, monitoring of activity in Worldpay work locations, and execution of backup and storage procedures	Worldpay relies on: • Worldpay's legitimate interests in protecting its rights, the integrity of Worldpay services, operations, facilities and systems, and preventing fraud or the misuse of Worldpay services.
Preventing, detecting and assisting in the prevention, detection or prosecution of:	Crime, including fraud, sanctions offences and money laundering	Worldpay relies on: • Worldpay's legal obligations under UK, EU or EU Member State law; • Worldpay's legitimate interests in conducting sanctions and anti-money laundering screening, and meeting non-UK, EU or EU Member State legal or regulatory requirements; and • Worldpay's legitimate interest in protecting and enforcing its rights and property.
Monitoring, auditing, and reviewing:	Communications and information on company systems, including email and website usage Compliance with company policies, procedures, and processes Activity in company work locations	Worldpay relies on: • Worldpay's legitimate interests in protecting the integrity of Worldpay services; and • Worldpay's legitimate interests in protecting and enforcing its rights, protecting the integrity of Worldpay services, operations, facilities and systems, and staff, and preventing fraud or the misuse of Worldpay services.
Preparing for, defending, participating in or responding to:	E-discovery requests for information Litigation or potential litigation and other types of dispute resolution (including complaints)	Worldpay relies on: • Legal obligations to participate in legal or complaints processes under UK, EU or EU Member State law; • Worldpay's legitimate interests in participating in legal or complaints processes under non-UK, EU or EU Member State law, regulatory or industry requirements; and • Worldpay's legitimate interests in protecting and enforcing its rights.

Purpose of processing		Legal ground(s) for use
Communicating and sharing of information with FIS companies or potential or actual acquirers of FIS companies or businesses for:	Internal administration and business management and planning purposes	Worldpay relies on: • Legal obligations relating to audit, tax, or compliance requirements under UK, EU or EU Member State law; and • Worldpay's legitimate interests to structure its business appropriately and to meet non-UK, EU or EU Member State requirements relating to audit, tax, or compliance.
Processing and administering:	Tax and other required withholdings	Worldpay relies on: • Legal recordkeeping and reporting obligations under UK, EU or EU Member State law; • Worldpay's legitimate interests in protecting its rights and meeting non-UK, EU or EU Member State recordkeeping and reporting requirements; and • The need to process personal data to fulfil contractual obligations.
	Reimbursements for business travel and other reimbursable business expenses	
	Invoices, payments, cash balances, and accounting	

Categories of data

With respect to data subjects whose personal data is processed by Worldpay for the purposes of the collection of accounts receivable, the processing of accounts payable, sales, marketing, vendor and customer relationship management purposes, the processing may concern the following categories of data.

Data Category	Example
Advice, opinions, and other comments	Engagement surveys, exit interviews.
Bank and financial details	Payment and/or expense reimbursement; direct deposit banking information, credit card information, wire clearing information, bank account number and sort codes, invoicing details, and payment details.
Business travel and movement data	Travel data, including travel schedules, lodging, conveyance, meals, and other expenses.
Grievance data	Complaints, tribunal data.
Information recorded on or in company systems, equipment, or documents	Emails, text messages, web site usage, voicemail recordings, calendar or diary entries, correspondence, including Personal Information included in or on company systems, equipment, or documents by the Data Subject.
Access records	Dates, times, and locations of entry and exit from controlled facilities and systems, computer and system logon/off audit trails.
Organizational data	Name, company structure, organizational charts, reporting relationships, titles, work contact details, email, accounting code details.

Personal details and contact information	Name, gender, birth date, home and business address, phone numbers, email, government-issued identification numbers, identification numbers issued by or on behalf of the company, signatures, handwriting.
Photo, video, or audio recordings	Information collected by security systems, closed-circuit television, profile photographs, voice mail, recorded trainings, conferences, or marketing materials.
Reports of disputes, defaults, or policy violations	Records of oral, written, email, telephone or similar reports pertaining to alleged and confirmed staff misconduct, contract issues, payment defaults, audits, or violations of company policies.
Talent, education, and training details	Education, skills, work experience, prior employment, training, language skills, technical skills, educational background, professional certifications and registrations, membership in professional bodies and organizations.
Work schedule data	Planned and actual working times.
Workplace safety data	Reports, photographs, video recordings.

Sensitive data

In some jurisdictions, personal data that is considered “sensitive personal data” or “special categories of data,” under applicable laws may be subject to more stringent protection and limitations on use than other personal data. What is considered “Sensitive Personal Data” varies by country, but generally includes information relating to a person’s sex life or sexual orientation, racial or ethnic origin, alleged or actual criminal offense, physical or mental health or condition, trade union membership, political opinions, religious belief, or genetic data.