

Comprehensive Privacy Notice

INTRODUCTION

Please read this notice carefully to understand our policies and practices regarding your personal information and how we will treat it. For a short-form summary, please click [here](#). California residents can find more specific information in the “California Consumer Privacy Addendum”. Quebec residents can find more specific information in the “[Quebec Privacy Notice Addendum](#)”. Contact Us details are provided at the end of the notice for feedback or any privacy enquiries you may have.

This notice applies to the companies that are part of the Paysafe Group, which use different trading names in different territories and the list of Paysafe companies that collect or process personal information according to this notice can be found at the end of this document. The reference to Paysafe (including “we”, “us” or “our”) includes those companies and all relevant group affiliates. This notice will not override any rights provided to you under the local privacy and data protection laws which apply in your jurisdiction.

References to “you” in this notice are to the individual who is enquiring, accessing or applying to use the Services (as defined below) either on your own account or on behalf of a business (e.g. a merchant or other business customer or party), or in relation to representatives or third parties acting on your behalf. This includes, in relation to a customer or prospective customer of Paysafe, any sole trader and any principals, including the managing and financial directors, any other directors and officers, shareholders, partners and beneficial owners of a customer, as well as any member of staff or representative accessing or using the Services or providing or requiring information on behalf of a customer. A separate privacy notice applies to Paysafe employees and candidates.

Paysafe is committed to protecting your privacy and will take all appropriate steps to ensure that your personal information is treated securely and will be collected, used, stored, and disclosed in accordance with this notice. This notice (together with our terms of use applying to any specific services you may purchase or use) applies:

to the web portals features and services provided to you when you visit our websites, portals, or our payment panels our clients may use on their websites;

when you enquire, apply to use and/or use Paysafe’s products and services, either directly or via a third party, including any loyalty or reward schemes, whether points-based or otherwise (“Loyalty”), campaigns or additional optional services or offerings, such as prize draws, lotteries, competitions, or similar, as well as when you request changes to the services you are using;

to your use of software including terminals, mobile and desktop applications provided by Paysafe; and

to email, other electronic messages including SMS, telephone, web chat, website/portal and other communications (in any medium) between you and Paysafe.

Together these are all referred to in this notice as “Services”.

INFORMATION WE MAY COLLECT FROM YOU

We collect and process personal and non-personal information relating to you.

Personal information is information that can be used to uniquely identify a single person, either directly or indirectly. In general, we use the terms personal information and personal data interchangeably, unless when referencing a specific local law which defines the terms differently.

Paysafe also collects non-personal information or may anonymise personal information to make it non-personal. Non-personal information is information that does not enable a specific individual to be identified, either directly or indirectly. Paysafe may collect, create, store, use, and disclose such non-personal information for any reasonable business purpose. For example, Paysafe may use aggregated transactional information for commercial purposes, such as trend analysis and the use of data analytics to obtain learnings and insight around payment transaction patterns and usage.

To the extent that Internet Protocol (IP) addresses (or similar identifiers) are clearly defined to be personal information under any local law, and where such local law is applicable to the Services, we will manage such identifiers as personal information.

Please note that Paysafe provides services to both individual consumers and businesses and this privacy notice applies to both and should be read and interpreted accordingly.

SENSITIVE PERSONAL DATA

We may collect information about you that is of a more personal or confidential nature, such as so-called special category data or sensitive data. These types of information can relate to an individual's:

Racial or ethnic origin

Political opinions

Religious or philosophical beliefs

Trade union membership

Genetic data

Biometric data

Health data

Data that relates to an individual's sex life or sexual orientation

Data about criminal offences or alleged crimes

Data about an individual's location in real time

Local laws may prohibit or restrict the use of such data and require specific obligations to be met. Within Europe, GDPR will generally require a second lawful basis for such processing, such as, (a) your explicit consent, (b) for the purposes of the establishment, exercise, or defence of legal claims, (c) for reasons of substantial public interest, or (d) where processing is necessary for your vital interests or of another natural person.

COLLECTING YOUR INFORMATION

We collect the following information through the following means:

Information you give us: we receive and store any personal information (including financial information) you provide to us including when you (or your business) enquire for or make an application for the Services; register to use and/or use any Services; upload and/or store information with us using the Services; and when you communicate with us through email, SMS, a website or portal, or the telephone or other electronic means, e.g. in the context of contacting us about your account or transactions. Such information may reference or relate to you or your customers and includes:

Name including first name and family name, date of birth, age, email address, billing address, username, password and/or photograph, biometric information, address, occupation, nationality and country of residence, a copy of your identification, such as your driver's license or passport, your social security number and/or other government identification or registration data;

Card primary account number, card expiry date, CVC/CVV details (card security code), account numbers, account balances and the length of time you have maintained those accounts, bank and/or issuer details;

Information relating to any items purchased, including the location of the purchase, the value, the time, and any feedback that is given in relation to such purchase, including travel-related personal information when you or your customer are transacting for airline tickets or other travel related services;

Information about your use of the Services, such as information about how frequently you transact with us, your transactions and average transaction volume, account balances, and the

people and merchants to whom you send money and from whom you receive money and, where you provide consent, information from your contact list;

Points or rewards earned or redeemed in any Loyalty scheme;

Photos and videos taken during Paysafe events you have registered for, for distribution to event participants and in our promotional materials for future events; and

Any other information that you or your customer provide or is generated in the context of using the Services.

Where we are required by applicable regulations, we may additionally process the personal information of vulnerable customers. What constitutes a vulnerable customer differs in different jurisdictions and we take these variations into account. If you have questions about or need further information, please contact us via the Contact Us section below.

Information we collect about you automatically: Paysafe receives and stores certain information automatically whenever you interact with Paysafe, whether you open an account or undertake a transaction with us; for example, by way of “cookies” or similar technology. We also obtain certain information when your web browser accesses Services or advertisements and other content provided by or on behalf of Paysafe on other web sites, or when clicking on emails. Collecting this information enables us to better understand the visitors and customers who use and interact with Paysafe, where they come from, and how they use our services. We use this information for our analytics purposes and to ensure the delivery, optimisation and relevance of services for our visitors and customers. We may also use such information for regulatory purposes, our own due diligence checks, fraud, and risk management. This information includes:

Technical information, including the Internet protocol (IP) address used to connect your computer or device to the Internet, your login information, browser type and version, equipment type, time zone setting, browser plug-in types and versions, operating system platform, frequency and length of visits, and what links you click on. For fraud and security purposes, the use of proxy IP addresses is generally forbidden when linking to Paysafe systems;

Information about your visit or whether you opened an email, including your geolocation (this may include software and services we use to verify your address for regulatory or risk purposes by determining whether an address you indicate matches the IP address of your log-in device), the full Uniform Resource Locators (URL) clickstream to, through and from our 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) and methods used to browse away from the site page and any phone number used to call our customer service number.

Information collected through our applications: if you download or use mobile or desktop applications provided by Paysafe, we may receive information about your location and your device or the service you are using (including where a payment transaction takes place). Some devices allow applications to access real-time location-based information (for example GPS). Our mobile and desktop apps may collect such information from your mobile device or your computer at any time while you download or use our apps, if your device has real-time location data access enabled. Where required, we will always seek to notify you if it is our intent to collect real-time location information and, also where required by law, obtain your consent. We may use such information for regulatory purposes, our own due diligence checks, fraud, and risk management, to better understand transaction patterns and to optimise your experience.

Email and Other Communications: we may receive information about you and your use of Services when we communicate with each other, including when you open messages from us and from the use of electronic identifiers (sometimes known as “device fingerprints”), for example, Internet Protocol addresses or telephone numbers.

Information from Other Sources: we may receive information about you from other sources and add it to our account information, including when you apply to use the Services. For example, we work closely with, and receive information from, third parties such as business partners, banks and other financial institutions, merchants, subcontractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, third-party data brokers, government lists and databases, social media sites (including posting made by or about you or us), credit reference and fraud prevention agencies. Prior to onboarding any business or company for our Services, we will perform various screening measures as part of our due diligence, including Politically Exposed Person (PEP) and adverse media checks on business owners. Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations around the world require PEP and other checks to be undertaken because of the increased AML/CTF risk they present, whilst adverse media screening entails searching media outlets to ascertain whether any information is available from an AML/CTF, risk and/or compliance perspective that could have a bearing on our decision to provide our Services to you.

Credit reference and fraud prevention agency use is further explained below. We may also review public comments and opinions made on social networking sites (e.g., Facebook and Twitter) to better understand our customers and our provision and development of Services.

Information about other people: if you give us information about other people, you must have informed them in advance (for example, by giving them this privacy notice) and you must ensure you have the right to do so.

WHAT WE USE YOUR PERSONAL INFORMATION FOR

We may use and share the personal information we collect for the following purposes:

To provide our Services to you and your business, including fulfilling Paysafe's obligations to you or to financial or other institutions in connection with the Services we provide to you (and / or your business). In this context we record and track details of transactions you (and / or your customers) carry out in relation to the Services; analyse and report on your (and / or your customers') use of any Loyalty service; facilitate the collection or redemption of any points or other rewards currency in respect of any Loyalty programme; notify you about important changes or developments to our website or our goods and services;

To deliver, improve and develop our business, including without limitation to optimise our websites/portals, products, and services. This may include using information you insert into forms but do not submit to us, for example by using that information to optimise our website(s) and contacting you for customer services or marketing purposes in relation to that form. We can also use your personal information to develop and test new products and services including in our secure and controlled test environment, or occasionally in those of our suppliers. Such use may include machine learning or artificial intelligence (including personal data to train AI models), or similar technological solutions; To manage and enforce our rights, terms of use or any other contracts with you (and/or your business), including to manage any circumstances where transactions, rewards or points are disputed; manage, investigate, and resolve complaints; or recover debt or in relation to your insolvency;

To manage and mitigate our credit risks and terms of business. If you apply for one of our financial products, we may assess whether or not we wish to provide services to you. This may involve an assessment of your financial position (and / or of your business), to the extent this is provided for in the applicable terms of use. This credit check will also affect any linked parties such as directors, shareholders, and principals. We can do so by receiving and sharing information from and with credit reference agencies, fraud prevention agencies and similar. This credit check will also affect anyone with whom you have a joint account or similar financial association. If it is a joint application, and such link does not already exist, then one may be created. These links will remain until you file a "notice of disassociation" at the credit reference agencies to the extent that such disassociation is allowable. For your information, the agencies will record our enquiries which may be seen by other companies who make their own credit enquiries; and a "footprint" may be placed on your credit file, whether or not you are accepted as our customer. If you are a Director or hold a similar position, we will seek confirmation from credit reference agencies that the residential address that you provide is the same as that held by the relevant companies' registry (where applicable). In addition, where you take services from us, we will give information on how you manage your accounts to the credit reference agencies. If you do not repay any monies in full and on time, credit reference agencies will record the outstanding debt and may share this information with other organisations that perform checks like ours. Records generally remain on file at such agencies for 6 years after they are closed, whether settled by you or defaulted,

although the retention period may differ across different agencies and territories. If you would like further information on our use of credit reference agencies, please contact us;

We may also carry out other risk assessments, including but not limited to adverse media screening, in order to assess whether we wish to provide services to you and/or the business you represent;

To verify and re-verify your identity, prevent and/or detect fraudulent applications, financial crime, manage risk and protect ourselves, our customers and the integrity of the financial system, including any checks required by AML/CTF or other laws. For these purposes, we may process and/or disclose your sensitive personal information (sometimes known as special category personal data, including biometric data. When we seek to confirm your identity, our vetted third-party supplier uses biometric facial recognition technology to determine if your selfie image matches the photo in your ID and to perform anti-fraud checks. During this process, your biometric data is generated to create a digital map of your face to perform the face match. We will obtain your consent prior to processing your biometric data. Refer to the Biometric Data Processing, Retention and Destruction section for detailed information. If you want to know more about our policies in respect of your biometric data, or indeed our use of any other sensitive or special category personal data, you can reach us at the details provided in the Contact Us section.

To prevent, detect and prosecute fraud and other crimes and abuses of the financial system, or to assist others in doing so, including non-compliance with any terms of business and which may involve the sharing of any relevant or necessary information we have collected or inferred with third parties for such purposes. Paysafe participates in anti-fraud initiatives, which involve assessing you (and/or your customers) and monitoring your transactions and/or locations, to detect patterns requiring investigation or otherwise profile and assess the likelihood of fraud occurring or non-compliance with our or other's terms of business, including requirements relating to politically exposed persons (PEPs) and sanctioned individuals. We can do so utilising products and services from third parties. Further, if you provide us with false or inaccurate information about you, or we identify or suspect a fraud or a crime, we may share your information with fraud prevention agencies, law enforcement authorities and similar bodies, and we may decide to take legal action against you. We will only disclose your biometric data where we are permitted by law or where subject to a legal obligation to disclose, such as a court order or a similar request from law enforcement, judicial, or other authorities in connection with the prevention, detection and prosecution of fraud;

To contact you about your account, alert you to potential problems, and respond to any questions you send to us;

To manage risks, such as credit and foreign exchange risks, as well as to prevent or mitigate information security risk;

Where permitted by law, we may use information related to financial well-being and other credit or risk factors to make decisions on the pricing of our Services.

We may use personal data, including demographic information and your dealings and transactions with us, to create audience segments and deliver tailored marketing communications in respect of products and services you have requested, or we think may be of interest to you.

This profiling enables us to better understand customer preferences and improve the relevance of our marketing. Profiling may include automated processing to evaluate aspects such as interests or behaviour in your use of our services or how we may perceive such use. You may have the right to opt out of such profiling at any time.

Where required by law, we will seek your explicit consent or meet other legal obligations before engaging in profiling activities that produce legal or similarly significant effects.

If you no longer wish to receive marketing or promotional information from Paysafe, you can always object at any time by opting out. You can find more information on this in the section on “Your Data Protection Rights”.

To obtain your views on our goods, services and our website/s; in respect of marketing, market research and similar activities, we may use your personal information for such purposes whether or not you are accepted as a customer or continue to receive Services.;

In compliance with or as required under applicable law and regulations;

To comply with requests from law enforcement and regulatory authorities on public interest grounds or from commercial organisations with whom you have or have had dealings, to establish, exercise or defend legal claims, or to protect your vital interests or those of other persons. For example, to help those authorities or other organisations in the fight against crime and terrorism or to operate in compliance with their own terms of business; and

To comply with card scheme rules or any terms of business.

If you provide information to be published or displayed on public areas of the website/portal or transmitted to other users of the website/portal or third parties, you understand that such information can be used by any third parties accessing the information for any purposes. This information is posted by you at your own risk, and you must comply with the terms of use of such site.

DISCLOSURE OF YOUR INFORMATION

We do not disclose information which could identify you personally, to anyone except as described in this notice, as permitted or required by law, and/or for the purposes described in this notice, including:

Within the Paysafe Group to help us provide and optimise our services and for our own internal customer relationship management, analytical and reporting purposes;

To recipients/senders of a payment in the context of the specific relevant transaction (generally information is limited to full name and email address);

Credit reference agencies (where permitted under any terms of use or other contract) as described above. If you would like further information on how we use credit reference agencies, please contact us;

Fraud prevention agencies as described above, including Action Fraud, Financial Fraud Action and the Financial Fraud Bureau and other organisations who assist us in managing fraud and business risk;

Third-Party Credit and Financial Institutions (where allowed under any terms of use or other contract), including the credit institution where the sender or recipient (and their businesses, respectively) maintain their bank account(s) and the card schemes governing the issue and use of credit, debit, charge, purchase or other payment cards, alternative payment schemes and any other financial institutions who may process payments and who are not operating under Paysafe's control nor for whose actions or omissions Paysafe has liability;

Where we provide services through third parties such as Banks and other organisations, we may be required to disclose your information (including any 'know your customer' and 'source of wealth' information) with such organisations to assist their own regulatory obligations or risk assessments;

Third Party Service Providers, including suppliers who assist us with the provision of Services, including processing orders, fulfilling orders, processing payments, managing credit, security, sector and fraud risk, identity verification, and marketing, market research and survey activities carried out on behalf of Paysafe. Occasionally, we may utilise the services of third-party providers to assist with the provision of services that might require the use of your personal information, including for the purposes of live data testing and/or utilising machine learning or Artificial Intelligence and for which suitable security arrangements will be implemented;

To third parties who do not act under our instructions as a service provider (but will be subject to their own legal obligations to keep data secure), to facilitate provision of the Services. For example, banks and organisations who facilitate the trading of your stocks, crypto currencies (including crypto service providers), and other financial instruments, as well as merchants or

retailers for whom we provide payment processing services and from whom you have or may be receiving services;

To prevent and/or detect fraud, financial crime, manage risk and to better protect ourselves and our customers, it may need to process and disclose sensitive personal information (sometimes known as special category personal data) to third parties who help us in managing such risks, including identity verification;

Where we are required or permitted to do so by law. Paysafe may be required by law to pass information about you to regulatory authorities and law enforcement bodies worldwide, or we may otherwise determine that it is appropriate or necessary to do so. Such disclosures may also include requests from governmental or public authorities, or with commercial organisations with whom you may have had dealings and who are seeking to mitigate fraud or credit risk, or non-compliance with terms of business, or for the purposes of litigation or legal process, national security or where we deem it in the national or public interest or otherwise lawful to do so. Paysafe will not ordinarily challenge the serving of court or similar orders requiring disclosure;

Business transfers. Paysafe may buy or sell business units or affiliates. In such circumstances, we may transfer or receive customer information as a business asset. Without limiting the foregoing, if our business enters a joint venture with or is sold to or merged with another business entity, your information may be disclosed to our new business partners or owners. In these circumstances we will inform the recipient that your information should be treated in accordance with the standards described in this notice; and

With your permission, your information may also be used for other purposes for which you give your specific permission.

Except as necessary for the performance of its services and as described above/attached, Paysafe does not sell, rent, share, or otherwise disclose personal information about its customers to third parties for their own third-party marketing use without meeting any necessary legal obligations (e.g., consent, opt-out, or as otherwise permitted by law). The California Consumer Privacy Act uses a very wide definition of data “sale” and California residents should read the “CCPA” section below in respect of data sale.

FRAUD PREVENTION AGENCIES

The personal information we have collected from you will be shared with fraud prevention agencies 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 or finance. Fraud prevention agencies can hold your personal data for different periods of time. If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services or financing you have requested, or we may stop providing existing services to you. A record of any fraud or

money laundering risk will be retained by us and the fraud prevention agencies, and may result in others refusing to provide services or financing to you.

If you are a resident of the UK, your personal information will be shared with Cifas. Further details of how your information will be used by us and Cifas, and your data protection rights, can be found [here](#).

HOW DO WE WORK WITH OTHER SERVICES AND PLATFORMS

Where available, you may be able to connect your Account with a third-party account or platform. For the purposes of this Privacy Statement, an “account connection” with such a third-party is a connection you authorise or enable between your Account and a non-Paysafe account, payment instrument, or platform that you lawfully control or own. When you authorise such a connection, Paysafe and the third-party will exchange your Personal Data and other information directly. Examples of account connections include:

connecting your Account to a third-party data aggregation or financial services company, if you provide such company with your Account log-in credentials; or

using your Account to make payments to a merchant or allowing a merchant to charge your Account.

If you create an account connection, we may receive information from the third-party about you and your use of the third-party’s service. If you connect your Account to a third party, we may have access to your account balance and transactional information, such as purchases and funds transfers. We will use all such information that we receive from a third-party via an account connection in a manner consistent with this Privacy Notice.

Information that we share with a third-party based on an account connection will be used and disclosed in accordance with the third-party’s privacy practices. Before authorising an account connection, you should review the privacy notice of any third-party that you authorised to have an account connection that will gain access to your Personal Data as part of the account connection. For example, Personal Data that Paysafe shares with a third-party account or platform such as a social media account may in turn be shared with certain other parties, including the public, depending on the accounts or platform’s privacy practices.

MONITORING

We may monitor or record telephone calls, emails, web chat or other communications with you for regulatory, security, quality assurance or training purposes. When visiting our offices, CCTV, access control systems and/or other monitoring systems may be in operation for security reasons and for health and safety and office management purposes and we may use machine learning, AI

or other technologies (including those provided or developed by third parties) in respect of such monitoring.

WHERE WE STORE YOUR PERSONAL INFORMATION

We, our service providers, and other parties with whom we may share your personal information (as described above) may process your personal information in territories that are outside the European Economic Area (“EEA”) or otherwise outside of the territory in which you reside. It may also be processed by staff (ours or that of our suppliers) operating outside the EEA or the territory in which the personal information was collected. Such staff may be engaged in, among other things, the fulfilment of orders, the processing of payment details and support services in provision of the Services. These countries may have data protection standards that are different to (and, in some cases, lower than) those of the territory in which you reside.

In these circumstances, we will take appropriate steps to protect your personal information in accordance with this privacy notice and applicable data protection laws; including using any appropriate safeguards required by law to ensure that any international data transfers are lawful. Paysafe generally uses “[Model Clauses](#)” as approved by the European Commission when contracting with third-party data recipients outside the EEA who are receiving data from within the EEA for the purpose of processing personal information transferred outside the EEA.

HOW WE KEEP YOUR PERSONAL INFORMATION SECURE

We have implemented technical, physical, and organisational/administrative measures designed to secure your personal information from accidental loss and from unauthorised access, use, alteration, and disclosure. These measures include:

Written information security program;

Appointed a Chief Information Security Officer (‘CISO’) and team to oversee, implement and enforce the information security programme;

Appointed a Chief Privacy Officer (‘CPO’) and team to oversee, implement and enforce the privacy programme;

Continuous vulnerability assessment and monitoring;

Having information security risk management policies and procedures in place;

Having an established incident response plan;

Access controls on information systems, designed to authenticate users and permit access only to authorised individuals;

Restricting access to physical locations containing personal information only to authorised individuals;

Securing all personal information, both in transit and at rest;

Multifactor authentication for all staff accessing personal information;

Maintaining audit trails relating to internal and external access to and modifications of personal information;

Adopted secure development practices for in-house developed applications;

Performing information security and privacy due diligence on third-party service providers;

Performing security and privacy awareness training on a regular basis.

The safety and security of your information is also dependent upon you. If we have given you (or if you have chosen) a password, passphrase or access code for access to certain parts of our website/portal or mobile applications and similar, you are responsible for keeping this password, passphrase and/or access code confidential. You must not share your password, passphrase and/or access code with anyone. You must ensure that there is no unauthorised use of your password, passphrase and access code. Paysafe will act upon instructions and information received from any person that enters your user id and password/passphrase and you understand that you are fully responsible for all use and any actions that may take place during the use of your account, unless otherwise mandated by law. You must promptly notify Paysafe of any information you have provided to us which has changed.

The transmission of information via the internet is not completely secure. Although we will do our best to protect your personal information, we cannot guarantee the security of your information transmitted to our site, unless you are communicating with us through a secure channel that we have provided. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

HOW LONG WE RETAIN YOUR PERSONAL INFORMATION

We will retain your personal information for as long as needed or permitted dependent on the context and purpose for which it was collected, the type of information and in compliance with applicable local laws or regulations.

This means that when using our Services, we will retain your personal information as necessary for the provision of the services and for any linked legitimate business purpose. This includes the use and retention of your personal information when you commence an application for our services, irrespective of whether you complete such application or are accepted as a customer. For example, account data is generally retained for up to 7 years after the closure of the account, to align with statute of limitation periods in the event of complaints or legal disputes. We may also be legally required to retain information, for example under anti money laundering or bankruptcy laws or where required by law enforcement or similar government agencies. Please note that the

relevant retention terms may vary per jurisdiction and some regions (e.g. DACH, LatAm) or laws extend retention to 10 years. Refer to the Biometric Data Processing section below for information about our retention of your biometric data.

We will retain personal information as evidence of our dealings with you regardless of whether there were any financial transactions, for audit and compliance practices, to manage any queries or disputes, including to defend or initiate any legal claims. We can also continue marketing and sending you direct marketing, subject to local laws and where you have not objected to such marketing.

We may also use data minimisation techniques to better protect your information, known as pseudonymisation. Once your information is no longer needed, we may anonymise or aggregate it with other information to make it unidentifiable, as an alternative to deletion.

YOUR DATA PROTECTION RIGHTS

Depending on your jurisdiction or country of residence, you may have one or more of the following rights:

Right to be informed: including by being provided with this notice.

Right to access: request a copy of the information we hold about you.

Right to erasure: request deletion of your information

Right to restriction: request we restrict the processing of your information.

Right to rectification: request we rectify certain information we hold about you.

Right to data portability: request that we provide you or another organisation with an electronic copy of the information you provided to us.

Right to object: request we stop processing your personal information.

Right to opt-out of marketing: remove your information from our marketing database.

Rights related to automated decision-making including profiling: see section “Automated Decision Making” below.

Right to opt-out of the sale of your data

These rights may apply under several different regulations, for example, the General Data Protection Regulation, generally applicable to EEA residents. Rights applicable to California residents under the California Consumer Protection Act, as amended by the California Privacy Rights Act, are outlined in the California Consumer Privacy Addendum below.

Furthermore, such rights may be qualified or restricted. For example, we may not be obligated to grant your request as we may be required by law to continue its processing, or to file a complaint or our legitimate interests may override your request for deletion. Similarly, we are unable to delete your information if you want to continue using our Services, or where such information is necessary to record our contractual dealings; it is required by law (for example, the retention of anti-fraud or “know your customer” identify and verification requirements); or for the purpose of defending or asserting legal rights and legal actions.

When you cease your relationship with us and stop using our services, we are permitted by law to retain your information for a period to evidence our dealings with you, as explained earlier. This will be in accordance with our internal retention policies and procedures. For more information on retention of data, please refer to the relevant section within this Notice.

To the extent that GDPR applies, when you give us consent to use your personal information, you can withdraw it any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent. For example, you can stop any marketing communication we send you by clicking on the “unsubscribe” or “opt-out” link in the communications you receive, or according to the instructions that we provide every time, but we will continue to send you operational or service messages in relation to your Services.

If you make a data complaint and you are not satisfied with our initial response or would like to challenge it, please don’t hesitate to contact us again. You always have the right to complain to a data protection authority if you are dissatisfied with our collection and use of your personal information. For more information, please contact your local data protection authority. Also, you may be able to commence a court action to claim compensation for damage or distress caused by our failure to comply with data protection legislation.

If you want to know more about your rights, or you want to exercise them, please visit [our dedicated rights page on our Paysafe website](#). Here you can submit a rights request directly to the relevant team, Alternatively, you can reach us at the details provided in the Contact Us section.

AUTOMATED DECISION MAKING

In some instances, our use of your personal information may result in automated decisions being taken (including profiling) that legally affect you or similarly significantly affect you.

Automated decision-making means that a decision concerning you is made automatically based on a computer determination (including the use of software algorithms, or artificial intelligence (AI) models or otherwise based on machine learning), without our human review. For example, we use automated decisions to complete credit or risk assessments on you when you apply for certain Services or to carry out anti-fraud and/or money laundering checks, as explained in the section ‘What We Use Your Personal Information For’. Such assessment will likely involve multiple

data points, including your address country, the security of your credentials and your use of our products, additional to the data points set out in the section 'Collecting Your Information'. The consequences for you may be our refusal to provide services or to provide services only on specific terms, including that you provide additional identity verification, proof of wealth and/or source of funds.

We have implemented measures to safeguard the rights and interests of individuals whose personal information is subject to automated decision-making. In addition, where required by applicable law, when we make an automated decision about you, you have the right to contest the decision, to express your point of view, and to request a human review of the decision. These rights apply in the EEA and in other jurisdictions where similar protections are provided by law, and we shall comply accordingly. To exercise this right, please complete our [dedicated rights form](#) or contact us via the details provided in the 'Contact Us' section.

AI and Machine Learning

In the delivery of our Services, we may utilise machine learning, artificial Intelligence (AI) or similar technological solutions. Where we adopt AI or other technologies, we will ensure compliance with applicable law and that such technologies are utilised in an ethical and non-discriminatory manner in respect of any characteristics protected under law.

AI Model development

To maintain and improve the accuracy of our fraud and AML/CTF controls and manage credit risk, we may use historical transaction data and known risk indicators (including data obtained from credit reference agencies where lawful to do so) to train, test and refine our AI models. Where feasible, we consider removal of direct identifiers and/or use aggregated data before using it for model development and apply strict access and security controls. This processing supports our legal obligations, our legitimate interests in identifying activity that may present a risk, and the wider public interest in maintaining secure and reliable financial services.

Biometric Data processing, retention and destruction

Biometrics refers to data derived from body measurements and calculations related to biological and human characteristics, used to recognize, or verify the claimed identity, of individuals. Paysafe may utilize Biometrics for identity verification during account opening and for re-verification when using certain Services, to enhance the security of your information and manage fraud risk. All processing of Biometric Data complies with relevant laws, including GDPR, the Quebec Information Technology Act 2001, the Illinois Biometric Privacy Act (BIPA) and applicable US state laws. Relevant definitions are as follows:

Biometric Data is the collective term for biometric identifiers and biometric facial templates:

biometric identifier is a scan of face geometry (distinct from the Selfie, as below).

biometric facial template/template is a mathematical representation of unique facial biometric characteristics generated by analysing and measuring scans of face geometry.

Biometric Facial Recognition is a comparison of biometric facial templates from submitted facial images, to perform a face match.

Selfie means a photographic image of your face taken by you and submitted by you (a Selfie is not Biometric Data).

How we use and store Biometric Data

Initial identify verification

To confirm identity on account opening or increase transaction limits, we obtain your consent for our supplier, Jumio, to perform Biometric Facial Recognition checks to match Selfies against ID documents and to detect and prevent fraudulent applications.

Biometric re-verification

Where you have completed the initial identity check and we need to re-verify you, with your consent, a new Selfie will be compared to the original using Biometric Facial Recognition; your biometric facial templates are generated momentarily and then deleted.

Biometric re-verification: paysafecard Instant Gifting

For paysafecard Instant Gifting, you can consent to store a biometric facial template for secure fund transfers between you and other paysafecard users. Biometric Facial Recognition checks compare a new Selfie against your stored biometric template and against biometric templates recorded for other paysafecard customers to authorize the transaction.

Consent withdrawal and retention

You can withdraw your consent for Biometric re-verification via the settings section of your mobile app or online account by switching the Biometrics consent toggle off. You will have to use our manual identity re-verification process, which is slower. Refer to the Biometric section of the settings in your account profile for details.

If consent is withdrawn and we do not identify fraud, the permanent deletion of your Biometric Data will take effect 4 months after your deletion instruction to satisfy our fraud verification measures. If fraud is suspected or detected, it will generally be retained for 2 years, up to a maximum of 3 years; which may be extended if there is an ongoing fraud or law enforcement requirement. If consent is withdrawn, the Selfie will no longer be used for Biometric Facial Recognition but will be retained in accordance with record retention rules in place within the applicable jurisdiction in which we operate

Destruction and disclosure

If you do not actively use your account after 3 years of registering for Biometrics and fraud is not suspected or detected, your Biometric Data is deleted, and you will need to re-register for the Service; your Selfie will be retained as per our retention schedule.

Paysafe respects and protects every person's confidential and sensitive information. Unless there is a valid warrant, court order, subpoena or other similar notice issued by a court of competent jurisdiction, Paysafe will: (i) comply with the retention schedule outlined and (ii) not disclose or otherwise disseminate any Biometric Data obtained from an individual's ID document and/or Selfie.

LEGAL BASIS FOR PROCESSING

Paysafe will only process your personal information in compliance with the law. Such laws vary across different territories and further specific information is available on request. In general, Paysafe will either process:

Based on your consent, for example to send you marketing messages about products and services in accordance with your interests and preferences, where such consent is required by law;

Where necessary for the performance of, or entry into, any contract we have with you, for example, to provide you with the Services you have subscribed – in that context, we need that information because otherwise we would not be able to provide the Services to you. For example, if we are required to verify your identity and you do not supply us with the relevant information, we may be unable to open an account for you;

Where Paysafe has a legitimate interest to process data, subject to such processing not overriding your own rights and freedoms in objecting to such processing. For example, to keep you informed about your use of the Services, improve and develop the Services and manage risk and fraud (including, for example, the use of your information to train our AI models), conduct online advertising or other marketing activities, as well as manage and enforce any claim or dispute;

Where Paysafe has a legal obligation to collect, use and/or disclose your personal information or otherwise needs your personal information to protect your vital interests or those of another person. For example, when necessary to comply with the rules imposed by our or other applicable regulators or similar bodies; or

Exceptionally, we may share your information with a third party when necessary, in the public interest, for example, when law enforcement agencies or other third parties with whom you may have had dealings request information to investigate a crime or otherwise a breach of third-party terms of business.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal information for any specific processing activity, please contact us via the Contact Us section below.

DO NOT TRACK & GLOBAL PRIVACY CONTROL SIGNALS

Some browsers and browser extensions support the Do Not Track (“DNT”) or Global Privacy Control (“GPC”) browser controls that can send a signal to the websites you visit indicating your choice to opt-out from certain types of data processing, including data sales. Upon the detection of GPC signals/ DNT browser request we will make reasonable steps to respect your choices as required by applicable law.

COOKIES

Please also refer to our [Cookie Policy](#) for details on how we collect, use, or disclose information in respect of cookies and similar technology. Otherwise, please contact us via the Contact Us section below.

CHANGES TO OUR PRIVACY NOTICE

We may, from time to time, change our privacy notice. If we make material changes to how we treat your information, we will notify you through a notice on this website/portal. The date the privacy notice was last modified is stated on this notice. Please ensure you periodically visit our website/portal and this privacy notice to check for any changes. However, if we are required by law to give you advance notice of any changes to this privacy notice and/or seek your consent to changes in our uses of your personal information, then we will do so.

LINKS TO THIRD PARTY SITES

Our site may, from time to time, contain links to and from the websites of third party networks, advertisers, and affiliates. If you follow such a link, please note that these websites have their own privacy and cookies policies and Paysafe does not accept any responsibility or liability for these third-party websites.

GLOBAL NOTICE

This notice is global in scope but is not intended to override any legal rights or prohibitions in any territory where such rights or prohibitions prevail. In such event, the rights and obligations set out in this notice will apply, subject only to amendment under any applicable local law having precedence.

EU REPRESENTATIVE

The companies of the Paysafe Group that are based outside the EEA have elected as their EU representative the following entity: Paysafe Bulgaria EOOD, 90, Tsarigradsko shose blvd, Sofia,

1784, Bulgaria. You can reach the EU representative using the contact details provided under the Contact Us section below.

UK REPRESENTATIVE

To the extent required under The European Union (Withdrawal) Act 2018 or other legislation in respect of “Brexit” the companies of the Paysafe Group that are based outside the United Kingdom have elected as their UK representative the following entity: Skrill Holdings Limited, 25 Canada Square, London, England, E14 5LQ, United Kingdom. You can reach the UK representative using the contact details provided under the Contact Us section below.

CONTACT US

All comments, queries and requests relating to our use of your information are welcomed. If you wish to exercise any of your rights, you may complete our dedicated [rights form](#). Alternatively, you may exercise your rights by contacting us on the details provided below. For further information as to the applicable Paysafe group companies to which this notice applies, you should write to the address below, marked FAO Privacy Department or contact us; but we do seek to maintain updated details in the list set out at the bottom of this notice.

Paysafe’s Group Data Protection Officer and Deputy are as stated below and can be contacted using the contact details provided under the Contact us section above or at the address below:

Mr Derek A Wynne

Mr Simon Brown (Deputy)

Paysafe, 2 Gresham Street, 1st Floor, London, United Kingdom, EC2V 7AD

California Consumer Privacy Act (CCPA)

If you are a California resident and use our consumer Services, you may have certain rights under the California Consumer Privacy Act (CCPA) (as amended by the California Privacy Rights Act 2022, aka CPRA) which are described below.

Please be advised that this notice supplements and should be read in conjunction with the Comprehensive Privacy Notice.

WHAT INFORMATION WE COLLECT

In the past 12 months, we collected the following personal information:

Identifiers, such as your name, age, date of birth, address and other contact details, a copy of your identification (such as your driver's license or passport), as well as your social security number and/or other government identification or registration data.

Professional or employment-related information, such as your occupation.

Internet activity, as set out in our [Cookies Notice](#), but including history of visiting and interacting with our Services, IP address, browser type, browser language and other information collected automatically.

Geolocation data to the extent we need to verify your location for regulatory or anti-fraud purposes depending on the Services provided and your use of them (for example, some laws may require us to identify your location if the use of any Services involves gambling).

Commercial information, such as information about your banking relationships, including account numbers, debit and credit card numbers, account balances, and the length of time you have maintained those accounts.

We collect this personal information to underwrite and set up your account and for the purpose of providing our Services to you.

"Do Not Share or Sell My Personal Information"

In the past 12 months, we shared with third parties any of the information described above for our business purposes, e.g., with our affiliates or in relation to using a service provider to assist us in providing Services to you. The categories of such service providers are described in the Disclosure of Your Information section.

We do not share your personal data directly with third parties for their own marketing purposes in exchange for monetary consideration. However, we do engage in Interest-Based Advertising and related activities, where we allow third parties to place cookies, pixels, and trackers on our sites to collect personal data in association with the delivery of personalised ads, or targeted advertising.

This may be considered a “sale”, “sharing”, or “targeted advertising” under the CCPA. In the past 12 months we have sold individual identifiers through our use of cookies and similar technology for users who do not opt out of such data use. We sell these identifiers to adtech providers and advertisers who provide targeted online marketing.

You can switch ‘on’ or ‘off’ your cookie usage in the online consent dashboard available via the ‘Cookie Settings’ link on all our websites and portals. To opt out of the sharing or sale of your personal information in our mobile applications, please use the ‘Privacy Settings’ tab available in your profile.

- Right to Limit Use and Disclosure of Sensitive Personal Information

If you are a California resident, effective January 1, 2023, you have a right to limit our use of sensitive personal information for any purposes other than to provide the services or goods you request or as otherwise permitted by law. To opt-out from such additional purposes, contact us via [this form](#) or by calling us at our toll-free number, +1 855 719 2087 (toll free number, available 9AM-7PM EST)

YOUR CCPA PRIVACY RIGHTS

You have rights that you can exercise in relation to your personal information. In particular:

Right to access: you may ask for information about the categories of personal information we have collected about you, the categories of sources from which your personal information has been collected, the business or commercial purpose for collecting or selling your personal information, as well as the categories of third parties with whom we may share or to whom we sell your personal information and the categories of personal information that have been provided to such third parties. You may also ask us for a copy of the specific pieces of personal information we have collected about you in a machine-readable format.

Right to deletion: you have the right to request the deletion of your personal information.

To the extent we sell your personal information you have the right to ask us to stop selling personal information about you to third parties or you can switch “off” your cookie settings using the online consent dashboard available via the ‘Cookie Settings’ link on all our websites and portals (which will have the same effect as opting out of sale of your personal information).

Right to nondiscrimination: you have the right not to be discriminated against because you have exercised any of your consumer’s rights listed above. In other words, we shall not provide a different quality of services to you because you have chosen to exercise one of your rights.

You may authorize a person to act on your behalf in relation to exercising these rights, but we may need to take certain steps to verify the request made is legitimate, i.e., that it is indeed coming

from you and that it is made on your behalf. For example, we may require your signed permission demonstrating that you have authorized the agent to submit the request on your behalf.

Please note that where we use and disclose personal information for purposes related to security, fraud detection and other similar purposes, some of your rights may be limited. As such, please consider that there might be cases where your request cannot be fulfilled. For example, as permitted by the CCPA, it is possible that we may not comply with a request to delete your personal information if we need that information for the purpose of detecting security incidents, or protecting against malicious, deceptive, fraudulent, or illegal activities, where such information is necessary to record our contractual dealings or your transactions (including evidencing nil transactions) or where required or otherwise permitted by law.

If you want to know more about your rights, or you want to exercise them, you can reach us at the details provided in the Contact Us section.

CONTACT US

California residents may also call us at +1 855 719 2087 (toll free number, available 9AM-7PM EST) or via the Contact us details provided above.

This Notice was last revised on 12th January 2026.

List of entities processing personal information

The Paysafe Group comprises Paysafe Group Holdings Limited, together with its subsidiaries. Below is a list of Paysafe Group entities that process personal information within the scope of Paysafe Group's Global Privacy Notice:

EcomAccess Inc / Ecom Access Inc. (Canada)

Foley Trasimene Acquisition Corp. II (USA)

IA Digital Marketing Inc / Marketing Numerique IA Inc (Canada)

NT Services Limited (Alberta) (Canada)

Openbucks Corp (USA)

Orbis Ventures S.A.C. (Peru)

Pi Jersey Holdco 1.5 Limited (Jersey)

PAYS Services UK Limited (UK)

PAYS Services UK Limited Indian Branch (India)

Paysafe Bermuda Holding LLC (Bermuda)

Paysafe Bulgaria EOOD (Bulgaria)

Paysafe Bulgaria EOOD - Irish Branch (Ireland)

Paysafe Direct, LLC (Delaware) (USA)

Paysafe Finance Canada Inc (Canada)*

Paysafe Finance PLC (UK)

Paysafe Financial Services Limited (UK)

Paysafe Financial Services Limited - Irish Branch (Ireland)

Paysafe Group Holdings II Limited (UK)

Paysafe Group Holdings III Limited (UK)

Paysafe Group Limited (Isle of Man)

Paysafe Holdings (US) Corp. (Delaware) (USA)

Paysafe Holdings UK Limited (UK)

Paysafe Holdings UK Limited - Irish Branch (Ireland)

Paysafe II Limited (UK)

Paysafe Limited (Bermuda)

Paysafe Merchant Services Corp. (USA)

Paysafe Merchant Services Inc. / Services aux commercants Paysafe Inc. (Canada)

Paysafe Newco Inc. (Canada)*

Paysafe Payment Processing Solutions LLC (Delaware) (USA)

Paysafe Payment Solutions Limited (Ireland)

Paysafe Payment Solutions Limited - Italian registration (Italy)

Paysafe Payments Asia PTE. Ltd (Singapore)

Paysafe Prepaid Services Limited (Ireland)

Paysafe Prepaid Services Limited - Gibraltar Branch (Gibraltar)

Paysafe Prepaid Services Limited - Italian registration (Italy)

Paysafe Technologies Inc. / Technologies Paysafe Inc. (Canada)*

Paysafe US Holdco II Corp (USA)

paysafecard.com Argentina S.R.L (Argentina)

paysafecard.com Wertkarten GmbH (Austria)

paysafecard.com Wertkarten GmbH - Irish Branch (Ireland)

paysafecard.com Wertkarten UK branch (UK)

paysafecard.com Wertkarten Vertriebs GmbH (Austria)

paysafecard.com MENA DMCC (Dubai)

paysafecard.com Mexico S.A.DE C.V (Mexico)

paysafecard.com Schweiz GmbH (Switzerland)

paysafecard.com USA Inc (USA)

Paysafecard On Odeme Servisleri Limited Sirketi (Turkey)

Paysafecard.com India Private Limited (India)

Prepaid Services Company Limited (UK)

SAFETYPAY CHILE, SPA (Chile)

SAFTYPAY S.A. (Ecuador)

Sabemul Beteiligungsverwaltungs GmbH (Austria)

SafetyPay Argentina S.A. (Argentina)

SafetyPay Brasil Holdco LTDA (Brazil)

SafetyPay Brasil Instituição de Pagamento LTDA (Brazil)

Safetypay Europe Entidad de Pago, S.A. Unipersonal (Spain)

SaftPay Inc (US) (USA)

SaftPay del Peru SAC (Peru)

SaftyPay Colombia S.A.S. (Colombia)

SaftyPay de Centroamérica S.A. (Costa Rica)

SaftPay Mexico S. de R.L. de C.V

SaftyPay Soluciones, S.A. (Guatemala)

Skrill Limited (UK)

Skrill Limited – Irish Branch (Ireland)

Skrill Limited Phillipines Rep Office (Philippines)

Skrill USA Inc (USA)

Viafintech GmbH (Germany)

Viafintech Zweigniederlassung (Switzerland)

* At the time of publication, it is intended that these entities will be amalgamated into Paysafe Merchant Services Inc. / Services aux commercants Paysafe Inc. (Canada) around the end of 2025.