

Convera Global Privacy Notice

Last update: August 25, 2025

Convera and its subsidiaries and affiliates (“Convera” or “we” or “us”) care about your privacy and are committed to processing your Personal Information in accordance with fair information practices and applicable data protection laws to better serve you. This Global Privacy Notice (“Notice”) describes how Convera collects, uses, stores, protects, discloses and shares your Personal Information when you use or interact with our Services, and the rights and choices about the way your information is collected and used.

The information set-out in this Notice will continue to apply even after the termination of your agreement with us for payment or other products and services. If we’ve provided you with separate or further information about how we collect and use your Personal Information for a particular product or service, those terms will also apply. We may also alter this Global Privacy Notice as needed for certain products and services and to abide by local laws or regulations around the world, such as by providing supplemental information in certain countries. This Global Privacy Notice is incorporated by reference in Convera’s Terms and Conditions. If you interact with us in a different context, e.g. as an employee, contractor or job applicant, separate terms might apply to that interaction.

Defined Terms

In this Policy, “Convera”, “we”, “our,” or “us” refers to the Convera entity responsible for the collection, use, and handling of Personal Information as described in this document. Depending on your jurisdiction, the specific Convera entity accountable for your Personal Information might vary. For a list of local Convera entities, please see the [“Convera Legal Entities”](#) Appendix.

“Services” refers to the products, services and applications that we provide under our Terms and Conditions and Addendums, websites (“Sites”) like [convera.com](#), and other Convera applications, including mobile applications and online services.

“Personal Information” or “personal data” means all information or data relating to an identified or identifiable individual. It does not include anonymous data, which cannot be linked back to an individual.

While data protection laws generally do not cover information related solely to legal entities (such as companies or other organizations), they do apply to Personal Information about individuals associated with those entities. Depending on the context, “you” or “your” means you or any person connected to you, namely any representative and other related people (including signatories, directors, ultimate beneficial owners, authorized users, your staff members) or any individual for whom we receive Personal Information to provide the Services.

1. Personal Information We Collect

We collect Personal Information about you when you use or interact with our Services and may use it along with other information collected or generated during our relationship with you from various sources described below. The Personal Information we collect depends on the context of the business relationship and your interaction with Convera.

We collect different types of Personal Information relating to you, which may include:

- Identifiers and account Information, for example your name, postal address, email address, telephone number, date of birth and nationality, user name and password, and user authentication data;
- Information about individuals’ affiliation with a legal entity, such as an individual’s role, and whether he or she is a beneficial owner, controlling person, authorized signatory or authorized user;

- Payment transaction information, which includes information about payers, remitters and beneficiaries for whom a payment or refund is submitted, bank account, routing number, amount and currency, other financial information;
- Client relationship data, payment and trade transactions data, and other financial data (e.g. data regarding creditworthiness), data included in relevant client documentation (e.g. record of advice) and other comparable data;
- Data we collect to comply with our anti-money laundering obligations and reporting obligations (including tax reporting, risk assessments, fraud prevention, identity verification, and sanction checks).

Depending on your relationship with us and to the extent permitted under applicable law, Convera may collect and process Government-issued identification numbers such as a national identification number (e.g., a Social Security Number, tax identification number, or passport number), state or local identification number (e.g., a Driver's License or other government-issued identification number), credit information, a copy of your government-issued identification card in relation to the purpose of identity verification and screening your Personal Information against lists of politically exposed persons ("PEP") and lists of persons or entities subject to sanctions, and Biometric Information (e.g., when you consent in the user experience through Touch ID/Fingerprint, face biometric and liveness detection to verify your identity with Convera);

- Other compliance data such as records maintained to demonstrate compliance with applicable laws; records related to client preferences, such as your opt-ins and opt-outs of marketing programs; and records related to data subject rights requests;
- Business-related information that helps us provide our Services to you, for instance how you use our Services, your interactions and communications to us during the duration of the relationship (such as orders, support requests, recordings of or information from calls, video and chats and other correspondence with our teams), bank and credit information, referrals and permissions to contact or marketing choices;
- Marketing and product or sales data, such as details of the Services you receive;
- Inferred and Derived Information by analyzing our relationship and transactional information (e.g. we may generate attributes and/or scores for marketing, security, risk or fraud purposes).
- Technical information, including the host from which you access the Internet, your IP address or device advertising ID, geolocation if enabled, information about your device (such as device properties, settings, applications, mobile application, browser and operating system software, social profile and network information, the date and time you access our websites and the address of the site from which you linked to our website when you visit us. We collect Personal Information on your online activities as described in the section titled "[Internet Technologies](#)."

To provide foreign exchange and payment instructions, or use other foreign exchange or payment services, you must provide certain information required by Convera to execute the transaction and to enable us to comply with our legal obligations associated with our foreign exchange and money transfer services. Failure to provide some of your Personal Information may affect our ability to provide our Services to you. This may include information about the form of identification used to send or receive a transaction (where required by law) including the identification or a copy of the identification document, transaction activity, bank account and payment information.

2. Sources of Personal Information

We may collect Personal Information about you from various sources, depending on our relationship and interaction with you. These sources may include:

- **Data that you give us**

This includes data you provide when you enroll in our Services, by filling in forms or by communicating with us, whether face-to-face, by phone, e-mail, chat, on-line or otherwise, or through your interactions with Convera affiliates and partners and other online Services and applications we offer (some of which may be managed by third parties on behalf of Convera). If you are sharing other individuals' Personal Information for business purposes – such as data belonging to your staff members or other related individuals – you confirm that these individuals have been informed about the use

of their Personal Information by Convera in accordance with this Notice. You also confirm that you have obtained all necessary consent, as required by laws and regulations applicable to you.

- **Data that we collect or generate about you**

This includes data we collect through your account, transaction forms, through the process of maintaining and upgrading our Services; through automated means such as communications protocols, email communications, recording calls with our representatives or call center, cookies or similar Internet Technologies; through your use of social media; and through your interest in Convera advertisements placed on third party sites.

- **Data we obtain from other sources**

We may also collect Personal Information from other sources such as your financial institution, including banks and non-bank financial institutions such as card processors, electronic money institutions and payment service providers, as well as our vendors, business partners, identity verification companies, payments and fraud risk management companies, law enforcement bodies, data aggregators, and commercial and public data sources.

3. How we use the Personal Information we collect

3.1 Legal basis

Convera may only use your personal data when the law allows us to. In most cases, our legal basis will be one of the following:

- **Contract necessity:** We use your Personal Information to provide our Services to you where processing personal data is necessary to carry out or enter into our agreement with you (for example, if the processing is needed for conducting foreign exchange and payment services);
- **Legal obligation:** We use your Personal Information for legal and compliance purposes where we have a legal obligation to process your data to comply with laws and regulations (such as reporting payment transaction details to domestic and foreign regulators, including your Personal Information, where such reporting is mandated by law, or collecting identification documents to comply with legal and regulatory duties related to anti-money laundering and counter-terrorist financing; detection, prevention and prosecution of fraud and theft as well as preventing illegitimate or prohibited use of our Services or other illegal or wrongful activity). This may further include using your Personal Information to validate and authenticate your identity and utilizing third parties to help us do so. This may also include establishing, exercising, or defending legal rights and claims of Convera and others, and monitoring and reporting compliance issues.
- **Legitimate interests:** We use your Personal Information for our legitimate business purposes (or the legitimate interests of one or more of our affiliates) where we have a legitimate reason to process your personal data that is reasonable when balanced against your rights and interests (for example, to understand how our Services are used and to improve them and for measuring marketing return on investment and brand satisfaction). This may include using your information to conduct market research surveys and to understand and improve your customer experience. We may also use your Personal Information to provide customer services and to help protect the security and integrity of our technology, systems, and services.
- **Consent:** We may process your Personal Information based on your consent. This includes consent for receiving marketing communications, or where otherwise required by applicable law. If we request your consent, we will inform you of the intended purposes for which your information will be processed. Where prior consent is not required under applicable law, we may send you marketing communications without express consent for such communications but will always provide you the ability unsubscribe from further such communications if you wish.
- **Substantial public interest:** Where we process sensitive or special categories of data (revealing or relating to someone's health, ethnicity, political views, religious beliefs, sexual orientation, or other protected characteristics) and that processing is in the substantial public interest (for example, to support vulnerable clients).

We will inform you when additional information is required to provide the Services you request or is required by law.

Even if you ask us not to use your data, we may continue to use your Personal Information in circumstances where (a) the law imposes an obligation on us; (b) we need to process it for the purposes of performing a contract; (c) we have a public interest to do so; or (d) we have a legitimate business reason for doing so (which may, in exceptional circumstances, override your interest that we no longer process your Personal Information).

3.2 Purposes for which we will use your Personal Information

Convera utilizes the Personal Information it collects for various purposes as set-out in this Privacy Notice.

What we use your Personal Information for	The legal basis for doing so
<p>To Determine if You are Eligible to Use our Services</p> <ul style="list-style-type: none"> To verify your identity and to check and refresh your information for accuracy, including verifying it with third-parties, to fulfil our legal obligations to conduct “Know Your Business”/“Know Your Customer” checks (KYB/KYC), including performing enhanced due diligence when applicable and screening your information against lists of politically exposed persons (“PEP”), sanctions and other lists. In some countries, as part of our KYB/KYC processes, we extract face scan information (known as “biometric information” or “biometric data”) from a selfie or video that you provide to compare with the picture of you on identity documents. If we do so, we will provide you with additional notices and obtain your consent where required by law. 	<p>Legal obligations</p> <p>Legitimate interests. It is in our legitimate interests to ensure the suitability of our clients.</p> <p>Substantial public interest (if we process Sensitive Personal Information to adhere to legal requirements that apply to us).</p> <p>Consent (for biometric data)</p>
<p>Provision of Services</p> <ul style="list-style-type: none"> To administer the business relationship, to provide Services to you or to a Convera client, including our Sites and other Convera applications, platforms and online services; to carry out accounting, reconciliation, vendor management, IT Operations and infrastructure management, inventory/asset management and analytics; to help you receive a personalized experience, to assist you in carrying out transactions; and for registering and accessing account information; In some countries we may have a legal obligation to provide you with certain Service features and functionalities. 	<p>Contract necessity</p> <p>Legal obligations</p>
<p>Security, Fraud Detection and Prevention</p> <ul style="list-style-type: none"> To promote safety, reduce financial risk and combat fraud across our Services; and fulfil other purposes which would be reasonably expected by you, or which are otherwise authorized or required under law. In some cases this may include collecting biometric data. We may use Artificial Intelligence (“AI”), including Machine Learning (ML) models and Generative AI (“GenAI”) to improve the efficiency and effectiveness of our financial crime and fraud prevention processes. For more information see “AI Systems” section. <p>To keep our anti-fraud measures effective, we can’t always share all the details about how we prevent fraud.</p>	<p>Contract necessity</p> <p>Legal obligation</p> <p>Legitimate interests. It is in our legitimate interests to detect, prevent, and investigate fraud, money laundering and other crimes to protect our business and our clients.</p> <p>Consent (for biometric data)</p>
<p>Compliance with Legal and Regulatory Obligations, Protecting our Business and Enforcing our Rights</p> <ul style="list-style-type: none"> To fulfil our legal obligations under applicable money-laundering regulations; To monitor the payments processed by us and to report suspicious transactions; To comply with other legal and/or regulatory requirements, including to respond to requests from public and government authorities, possibly outside your country of residence, upon demonstration of lawful authority; 	<p>Legal obligations</p> <p>Legitimate interests. It is in our legitimate interests to protect our business, clients and employees from harm.</p>

<ul style="list-style-type: none"> • To prevent, detect, or protect against actual or suspected fraud, unauthorized transactions, claims, liability, and financial or other crimes, including conducting or co-operating with investigations of fraud or other illegal activity where we believe it is reasonable and appropriate to do so; • To measure, detect and prevent the likelihood of financial, reputational, legal, compliance or business loss. This includes credit, operational and insurance risks; • To enforce our agreement with you and to protect our rights: this includes to verify information you provide to us, to keep track of the instructions you send to us, to take steps to recover amounts owed to us, including via insurance claims, to allow us to recover or limit damages that we may sustain and to allow a third party or a financial institution that incorrectly sent payments to recover payments received by you in error or due to fraud; to investigate, manage, and resolve complaints; to prevent, investigate and manage incidents; to handle and resolve legal disputes or for regulatory investigations; and in the event of a restructuring of companies or other mergers or acquisition. 	
<p>Maintaining and Improving our Services</p> <ul style="list-style-type: none"> • To provide support services – for example, to respond to requests, questions or concerns, and communicating with you for service-related purposes; • To recognize you and allow you to remain signed-in during your visit without having to re-enter your password; • To notify you of updates to the services, scheduled maintenance, security alerts and we may also hold training sessions, webinars and events; • For analytics, improvement and research: to perform analytics on understanding our clients, how they use our services and improving their experience; to understand, track and improve how we market and sell our services, including service testing, quality assurance and analytics; and to identify other possible service and product improvements (including profitability); • For internal operational, planning, audit, troubleshooting, data analysis, testing, research, statistical, and survey purposes; • We may use Artificial Intelligence (“AI”), including Machine Learning (“ML”) models and Generative AI (“GenAI”) to improve the efficiency and effectiveness of our services. For more information see “AI Systems” section. 	<p>Legitimate interests. It is in our legitimate interests to maintain, develop and improve our services to better serve our clients.</p>
<p>Data as a Product</p> <ul style="list-style-type: none"> • Where we collect data for another purpose, e.g. for delivery of Services, we may share such data or analytics results with third parties including other Convera entities where it is in our legitimate interest to do so. The data may be presented as research whitepapers, the delivery of client-specific information or other data insights to clients. • We may create anonymous, deidentified, or aggregate data from personal data we collect. We make personal data into anonymous, deidentified, or aggregate data by excluding information that makes the data personally identifiable, and use that anonymous data for our lawful business purposes. 	<p>Legitimate interests. It is in our legitimate interests to analyze, understand and create value and data insights related to our Services.</p>
<p>Marketing and Analytics</p> <ul style="list-style-type: none"> • Advertising: to deliver information specific to your interests on non-Convera websites and applications; • Analysis of promotions: to better understand the effectiveness of our promotional campaigns and whether you acted on our promotional messages; • Web traffic analysis: to determine whether you came to Convera from a banner advertisement or an Affiliate. • We may also gather analytics on website navigation and access to our marketing and promotional material using industry standard technologies to help us analyze and improve our marketing materials. 	<p>Legitimate interests. It is in our legitimate interests to let our clients know about our products and services which may interest them, to personalize marketing communications and to understand the effectiveness of our advertising.</p>

	Consent where we are required to collect your consent by law.
Understanding if You Require Specific Support <ul style="list-style-type: none"> In some countries, it's a legal requirement for us to proactively identify and assist vulnerable clients that may need extra assistance – for instance, if you have suffered a bereavement or are experiencing financial difficulties. 	<p>Substantial public interest (if we process your sensitive Personal Information to adhere to legal requirements that apply to us).</p> <p>Consent (where we are required to collect your consent by law).</p>

3.3 Profiling and Automated Decision Making

When providing you with our Services, in view of entering into a contract with you, including where we provide you with a credit line, we may make decisions about you by automated means. For example, we use technology that helps us conduct business-related checks, including identity verification and due diligence processes, screening against Politically Exposed Persons lists, sanctions lists, other lists where applicable to identify and mitigate risks associated with things such as money laundering and financing of terrorism.

We may also analyze and evaluate your data in an automated manner so as to create customer profiles and predict developments. These may in particular be used for business-related checks, advisory or financial services, the provision of offers and information that we, or our affiliates, may make available to you; and to help us identify the level of risk involved in customer or account activity (e.g. for credit, fraud or financial crime reasons).

We may also use, on a need basis, models and algorithms that are based on Artificial Intelligence and Machine Learning systems (collectively "AI Systems") for analyzing and extracting information, for automating or performing tasks, and the generation of new content including content in human language.

You have a right to certain information about how we make these decisions; you may also have a right to request human intervention and to express a view on any automated individual decision where such opportunity to express a view is required by law. Please refer to "[Your rights](#)" section below, for more information.

3.4 Recording of Communications

We may record and keep track of conversations you have with us – including phone calls, face-to-face meetings, letters, emails, live chats, video calls, and any other kinds of messaging, including by automated means, including using third-party systems, in order to comply with record keeping obligations, be able to reconstruct any trades with customers and use these recordings to check your instructions to us, assess, analyze and improve our service, train and coach our staff members, manage risk or to prevent and detect fraud and other crimes.

We enable you to exercise your rights as a data subject under applicable law with respect to these recordings as set out in this Notice. In the event that you request a copy of the recording, Convera may provide you with a redacted copy of the recording, or a (redacted) transcript of the recording, where appropriate, and as permitted under applicable law.

3.5 Internet Technologies

We use internet technologies like cookies, tags, pixels and web beacons on our Sites, in mobile applications or when you visit a third-party website for which Convera provides online Services for a variety of purposes, including, but not limited to those identified in the section titled [“Purposes for which we will use your Personal information”](#).

Convera has implemented the capability for the user to manage cookies on our websites. We will only read or write cookies based on your preference level. For more information on how Convera uses cookies please refer to our website.

3.6 Artificial Intelligence (AI) Systems

Convera may utilize technologies such as Artificial Intelligence (“AI”), Generative Artificial Intelligence (“GenAI”) and Machine Learning (“ML”) (“collectively “AI Systems”) which enable computer systems to automate or perform tasks that may process your Personal Information in connection with the Purposes outlined in the Global Privacy Notice. These technologies and tools help us, and our service providers, in internal business activities and for enhancing productivity, furthering security, risk or compliance systems, and promoting revenue generation through insight-driven decision-making.

How We Use AI Systems: Convera is committed to the ethical use of Personal Information in AI Systems and has developed processes and oversight for the development and use of AI Systems, including an AI Governance structure and AI Policy. Convera’s AI Policy establishes requirements for the responsible use, development, and deployment of AI Systems within Convera and provides a framework to help ensure compliance with applicable legal and regulatory standards while promoting uptake and innovation of AI technologies. This includes evaluating the Artificial Intelligence or Machine Learning technology or tool for its appropriateness, the sensitivity of the Personal Information processed, the impact on the rights and freedoms of individuals, and the potential for bias if they are being used to assist in decision-making. Outputs are also typically subject to human review and reviewed and amended by an individual for accuracy and completeness. Our use of AI Systems does not generally result in automated decisions with any material legal or similar effects. If our use of AI Systems has a material effect on an individual, we provide a specific notice and obtain consent where required under applicable data protection laws.

The examples listed below are not exhaustive and are subject to compliance with and to the extent permitted by applicable law:

- **Enhancing productivity.** AI solutions can generate significant process efficiencies across the enterprise. These solutions include:
 - Office Productivity SaaS (Software as a Service) tools that use Generative AI for search, document analysis and assistance, including data contained herewith, to assist with drafting, translating, generating content, and providing insights to facilitate and improve the efficiency and productivity of our Services;
 - Voice/video Meeting Productivity SaaS tools that use Generative AI for note taking, transcription and/or summarization of voice and video calls, which may include Personal Information, to increase the performance and efficiency of sales and operations and compliance monitoring;
 - Technology Management tools using AI/ML for streamlining workflows, automating repetitive tasks in product development and technology management processes;
 - Customer Support applications using AI/ML to improve the handling and response efficiency to customer support queries and cases and support decision-making.
- **Strengthening our Protections on Compliance, Risk, and Security.** Convera’s current use of risk, compliance and/or security systems or tools can be enhanced by the use of AI for strengthening our protective measures particularly in the case of risk, compliance, fraud and transaction monitoring and for improving the security of Convera IT systems and assets.

- **Creating Value through Recommendations for Our Clients.** Leveraging AI solutions to enhance our products and services. By using AI-driven recommendations, Convera can offer tailored solutions that more closely meet client needs and drive better outcomes.

3.7 Marketing

Convera will also, subject to your preferences, notify you of offers, promotions and updates regarding our products and Services. These may include offers by email, telephone, postal mail, social media and other communication or digital channels.

You can opt out of receiving marketing communications at any time. If you no longer want to receive marketing-related communications from us on a going-forward basis, you may opt out by following the instructions in the relevant electronic communication or by contacting us as described in the [“Contact Us”](#) section.

Please note that if you opt out of receiving marketing-related communications from us, we may still send you important service, administrative or transaction-related communications.

4. Information from Children

Convera does not provide our Services or products to children under the age of 18. Convera does not knowingly collect or maintain information from persons under the age of 18 other than for purposes of legal or compliance.

5. External websites

Convera's Website may be linked to or from third party websites. Convera has not reviewed, does not control, and is not responsible for the content or privacy practices employed by websites that are linked to or from our website. Convera does not assume responsibility for any of these sites, their content, or their privacy policies. Convera does not endorse third party websites or make any warranties about any information, software or other products or materials you may find there, or any results that may be obtained from using them.

For further information about liability towards external websites, please review our website Terms of Use.

6. Who Convera Shares Your Personal Information With

For any of the purposes listed in this Notice, Convera may disclose applicable Personal Information including, but not limited to, your name, contact information, national identification number, customer ID number, address, transaction details, patterns and bank account information to the following types of organizations or parties:

- **Convera group companies and affiliates**, including those listed in the section titled [“Convera Legal Entities”](#) which may assist in providing our services to you, improving our operations, and supporting business functions such as customer support, technology, marketing, fraud prevention and compliance.
- **Trusted third-party service providers and partners** (some of which may act as independent, separate data controllers who determine why and how they will process your data), such as:
 - Local licensed entities who are supporting, partnered with or receiving services from Convera;
 - Business Partners which may include Banks and other Financial Institutions we work with to provide our Services and facilitate our payment transactions or specific Services you have requested;
 - Cloud storage providers and other technology service providers, that provide hosting, IT services, operating systems and platforms, maintenance, and technical support to ensure our platforms and services function optimally;

- Vendors, payments processors, and data processors contracted to provide business and customer services;
 - Vendors and data processors contracted to help us validate the accuracy of the information provided by you and to authenticate your identity;
 - Fraud prevention agencies and providers of fraud prevention services and data analytics to manage risks related to security, fraud and identity;
 - Customer service, advertisers and advertising networks, based on your consent where applicable, including for conducting marketing, advertising, customer satisfaction surveys and market research on our behalf;
 - Independent third-party service providers and professional services organizations such as legal advisors, accounting services or independent auditors.
- **Authorized Third-Parties and Users:** Third parties and users that you have authorized to access your account and/or your account information in order to perform Services for you, such as account information service providers, payment initiation service providers, and authorized users.
 - **Business Transfers:** We may transmit Personal Information we possess in connection with a sale or transfer of all or part of our business.
 - **Regulators, law enforcement agencies, and public authorities,** including judicial and administrative courts: We may also disclose your Personal Information globally, as required or permitted by applicable laws and regulations, to regulatory and financial authorities, credit reporting agencies, law enforcement bodies, courts, governments or government agencies, to meet compliance and legal obligations or to assert or defend the rights and interests of Convera or others.

7. International Data Transfers

Convera has affiliates and service providers around the world. Convera may transfer your Personal Information to parties in countries outside the country, region or province it was collected, including but not limited to the United States, as permitted or required by applicable law, regulatory authorities, law enforcement and government agencies.

We may transfer and store information in the United States or within a region as required by local law and process it to fulfil our contract and the legal and compliance obligations which apply to our Services. We also store Personal Information we collect using cloud storage providers and other technology service providers located in the United States, European Union and other local data centers as applicable. To facilitate our global operations, information may be accessed by our staff (including those of outsourced partners) in other jurisdictions. Additionally, when you send or receive money to or from another country, we will also be required to share some Personal Information with that country as required or permitted by law. By using Convera's Services, you acknowledge that such transfers of information outside of your country or province of residence may occur. If you are a EEA, UK or Quebec resident, this means your Personal Information may be transferred outside EEA, UK or Quebec, including to service providers located outside your country or province of residence.

When transferring Personal Information to other countries we take measures to comply with data protection laws applicable to those transfers. In particular where a transfer is to a country with data protection regulations that do not offer an equivalent level of data protection to your country, we will take all steps reasonably necessary to ensure that your Personal Information is handled securely and in accordance with this Notice.

When a data transfer mechanism is mandated by applicable law we:

- Transfer to countries or recipients that are recognized as having an adequate level of protection for Personal Information under applicable law;
- Enter into EU Standard Contractual Clauses approved by the European Commission and the UK International Data Transfer Addendum issued by the Information Commissioner's Office with the data importer.
- Employ other lawful methods such as transfer mechanism or derogation available to us under applicable law.

More information about the third parties to whom we may transfer Personal Information, their locations, and the contractual arrangements in place to comply with applicable data protection laws can be provided to you if you send a request as indicated in the [“Contact Us”](#) section.

8. How We protect Your Personal Information

We take the safeguarding of your information very seriously and we endeavor to use organizational, technical and administrative safeguards that comply with applicable government laws and regulations to secure your Personal Information. We also endeavor to restrict information access to our employees, partners and representatives that need to know and we continuously educate and train our employees about the importance of confidentiality and privacy of customers' Personal Information.

We are regularly audited to confirm we remain compliant with our security certifications. As part of these audits, our security is validated by external auditors. You can find out more from our [Compliance and Legal](#) section on our website.

Despite our efforts, and as you probably know, the transmission of information via the internet is not completely secure. Although we do our best to protect your personal data, we cannot guarantee the security of your data during transmission. Third parties may unlawfully intercept or access transmissions sent to us or may wrongly instruct you to disclose Personal Information to them while posing as Convera.

Please contact us immediately in accordance with the [“Contact Us”](#) section, if you have reason to believe your Personal Information held by Convera may be at risk.

9. Data Retention

The Personal Information will be retained in accordance with statutory periods contained in regulations applicable to us.

We will keep the Personal Information for as long as you have a relationship with us and use our Services. We will continue to keep the information after the termination of our relationship or after you stop using our Services, for instance, to respond to enquiries and complaints, and as required by law and regulations. We will typically keep your information for no longer than the purpose(s) for which it was obtained, unless we have a legal or regulatory obligation to keep it for a longer period or retention is advisable for Convera's legal position (for example, regarding applicable statutes of limitations, litigation or regulatory investigations).

More precisely, we are subject to various retention and documentation obligations which are, inter alia, applicable pursuant to the provision of payment services and financial transactions including those in anti-money laundering, anti-terrorist financing and other laws applicable to us. The retention periods provided by those laws vary from five to ten years after the termination of the client relationship or last-executed transaction. Finally, the retention period will also be determined by the legal limitation periods that can be, for example, as set forth by the civil code, code of commerce, or other applicable statutes of limitations.

When we no longer need the information we will destroy it in a safely and secure manner, or fully anonymize it, in accordance with our internal policies.

10. Your Rights

Depending on the applicable laws of the jurisdiction in which you reside or are located, you may have the following rights:

- The right to know if we are processing your Personal Information and, subject to applicable law and certain limitations and exemptions, to ask us for a copy of your information free of charge. This may include the right to request a structured

and machine-readable copy of certain information you have provided to us. We may charge you a reasonable fee for providing the information, or not act upon your request, if the request is manifestly unfounded or excessive.

- The right to ask us to correct information about you that is incomplete, inaccurate or out-of-date.
- The right to ask us to delete certain information about you, to restrict certain uses of information relating to you, and to object to certain uses of it.
- The right to object to an automated decision, if the automated decision produces legal effects or similarly significantly affects you.
- The right to stop us from sending you marketing communications.
- To the extent we are processing Personal Information based on your consent, you may withdraw your consent as permitted by applicable law.

Additional rights may be provided through supplemental privacy notices in certain countries. Please refer to our section titled "[Specific Provisions](#)".

You may also have the right to lodge a complaint with a relevant data protection regulator or supervisory authority about our processing of Personal Information. When we receive a request, we may ask for additional information from you to verify your identity. In some situations, we may refuse to act or may impose limitations on your rights, as permitted by applicable law.

To exercise these rights, please visit our website, submit a request via the [Privacy Webform](#) or contact Convera through the section titled "[Contact Us](#)".

We endeavor to respond to your request within 30 days but response time may vary depending on the laws and regulations applicable to your request and we may be entitled to extend this period in certain circumstances. We will comply with your request to the extent required by applicable law.

11. Contact Us

If you have a question or complaint about how we handle your Personal Information, or want to exercise any of the rights explained above, you are welcome to contact us. Please do so in writing at privacymatters@convera.com or submit a request by completing this online form: [Privacy Webform](#). We will investigate your enquiry and generally respond to you in writing within 30 days of receipt.

Convera has appointed a Data Privacy Officer who is responsible for advising on and monitoring compliance with applicable data protection legislation and has a dedicated privacy office that can assist you in case of questions. If you want to reach the Data Privacy Officer specifically, please state this in your request or email.

To contact us via registered letter, please refer to the contact information in the Convera Legal Entities appendix, c/o Privacy Office. To contact us via a toll-free or local phone number, please refer to the contact section of our website.

12. Changes to This Notice

Convera reserves the right to modify this Global Privacy Notice. Updated Notices will be posted on our website when amendments occur and may include information on additional processing activities we intend to perform going forward. If we make changes to the Notice, we will let you know by posting the revised Notice with a new "Last Updated" date posted at the top of the Notice. Any changes to this notice will become effective when posted unless indicated otherwise. We therefore urge you to review this Global Privacy Notice regularly when using our Services to stay informed about our information practices and the choices available to you.

Specific Provisions

This Global Privacy Notice is supplemented by the following additional notices, depending on how you interact with us and where.

- [U.S. State Privacy Laws Supplementary Notice](#)
- [U.S. Consumer Privacy Notice](#)

Additionally, our [Cookie Policy](#) explains our practices regarding cookies, tags, and similar types of online data that we collect.

U.S. State Privacy Laws Supplementary Notice

We care about the privacy of our U.S. users and are committed to collecting, using, storing, protecting, disclosing and sharing your Personal Information in accordance with applicable U.S. laws.

This supplemental notice only applies to residents of certain U.S. States whose information is processed pursuant to applicable U.S. State law privacy requirements, including the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, “CCPA”), the Oregon Consumer Privacy Rights Act (“OCPA”), the Minnesota Consumer Data Privacy Act (“MCDPA”), other applicable U.S. State Privacy laws (collectively, “U.S. State Privacy Laws”). This supplemental notice to the Convera Global Privacy Notice is applicable to those U.S. residents, including residents of California and, in conjunction with the Global Privacy Notice, is intended to address the requirements of the U.S. State Privacy laws, including CCPA.

When you use our Services, we collect Personal Information about you as permitted by applicable laws and regulations. However, note that in the United States, payment transaction and other financial information Convera processes in connection with its Services may be regulated by existing federal or state financial privacy laws such as the Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA). U.S. State Privacy Laws generally recognize that, where such financial information is already protected by specific privacy law, these U.S. State Privacy Laws do not apply to this information. Depending on how you interact with us or our Services, we may provide supplemental privacy notices explaining our handling of your Personal Information subject to these other laws.

For more information about the Personal Information that may have been collected about you, please review our Global Privacy Notice to which this supplemental notice is appended.

If you are a U.S. Consumer under financial regulations (e.g. GLBA, CFIPA), please review our [U.S. Consumer Privacy Notice](#).

The section “**Collection of Personal Information**” below describes the categories of Personal Information subject to U.S. State Privacy laws that we may have collected or disclosed for business purposes in the past 12 months, the sources of the Personal Information, the business or commercial purposes for which we use or disclose the information, and the categories of third parties to whom we disclose the information for business purposes.

We retain your Personal Information for as long as needed, or permitted, based on the reason we obtained it (consistent with applicable law) and as described in the Global Privacy Notice (section titled [Data Retention](#)) and this supplemental notice. When deciding how long to keep your Personal Information, we consider whether we have an ongoing relationship with you, are subject to any legal obligations (e.g., any laws that require us to keep records for a certain period of time before we can delete them), or whether we have taken any legal positions (e.g., issued any legal holds or otherwise need to preserve the information). Rather than delete your data, we may also deidentify it by removing identifying details. If we deidentify the data, we will not attempt to reidentify it.

U.S. State Privacy Laws provide their residents with specific privacy rights, including the right to correct inaccurate Personal Information, delete Personal Information, and access Personal Information and other information about our Personal Information processing practices, including in a portable format. Some U.S. State Privacy Laws may also give their residents the right to appeal our decisions with respect to your privacy rights requests. As described further in the section “[U.S. States Privacy Rights](#)” below, U.S. State Privacy Laws may also give their residents the right to opt-out of having their Personal Information sold, processed for targeted advertising purposes, or used for profiling in certain contexts, as well as certain rights in relation to the processing of their sensitive Personal Information. Finally, U.S. State Privacy Laws may give their residents the right not to receive discriminatory treatment for the exercise of any of these privacy rights.

Collection of Personal Information

Convera may collect (and in the 12 months prior to the effective date of the Notice, Convera may have collected) the below Categories of Personal Information from the indicated Categories of Sources; this information may have been shared with the described Categories of Third Parties for the specified Business Purposes. Categories of Sources, Categories of Third Parties, Commercial Purposes and Business Purposes are further defined in the Global Privacy Notice and below.

Categories of Personal Information	Categories of Sources	Business and Commercial Purposes	Categories of Third-Party Recipients
Identifiers: contact information provided for example your name, postal address, email address and telephone number; date of birth provided; nationality provided, social profile and network information; IP address; device identifier; mobile ad identifier; cookies; beacons; and pixel tags	<ul style="list-style-type: none"> You Your Use of our Sites Affiliates, Subsidiaries or Vendors Third parties 	<ul style="list-style-type: none"> Performing the Services Auditing Security Purposes Quality Purposes and Safety Analytics Web Traffic Analysis Advertising Analysis of Promotions 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Our business partners Professional services organizations Data analytics providers Operating systems and platforms Advertising and social networks Government entities.
Commercial information: including use of our Services, communications with us, payment and transaction information, bank account, routing number, amount and currency, other financial information	<ul style="list-style-type: none"> You Your Use of Our Sites Affiliates, Subsidiaries or Vendors Third parties 	<ul style="list-style-type: none"> Performing the Services Auditing Security Purposes Internal R&D Short-term use Quality Purposes and Safety 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Our business partners Professional services organizations Data analytics providers Operating systems and platforms Government entities
Internet and Other Electronic Network Activity Information: including the host from which you access the Internet, information about your device (such as device properties, settings, applications, storage and usage information), mobile application, browser and operating system software, the date and time you access our websites and the address of the site from which you linked to our website when you visit us.	<ul style="list-style-type: none"> Your Use of Our Sites Affiliates, Subsidiaries or Vendors Social Media Networks or Publicly Available Sources Advertising Networks 	<ul style="list-style-type: none"> Performing the Services Authentication Auditing Security Purposes Quality Purposes and Safety Debugging Short Term Use Internal R&D Analytics Web Traffic Analysis Advertising Analysis of Promotions 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Our business partners, Professional services organizations Data analytics providers Operating systems and platforms Advertising and social networks Government entities
Geolocation Data: precise geo-location may be collected from your devices only if enabled	<ul style="list-style-type: none"> Your Use of our Sites 	<ul style="list-style-type: none"> Auditing Security Purposes Short-term use Internal R&D Quality Purposes and Safety 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Data analytics providers Operating systems and platforms

			<ul style="list-style-type: none"> Advertising and social networks Government entities
Audio, Electronic, Visual, or Similar Information: including call/video recordings if you interact with our customer service representatives.	<ul style="list-style-type: none"> You 	<ul style="list-style-type: none"> Performing the Services Auditing Quality Purposes and Safety Security Purposes Short-term use 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Data analytics providers Operating systems and platforms Government entities
Professional or employment information: including business information, employer information, contact emails, taxpayer ID numbers	<ul style="list-style-type: none"> You Your Use of Our Sites Affiliates, Subsidiaries or Vendors Third parties 	<ul style="list-style-type: none"> Performing the Services Auditing Quality Purposes and Safety Security Purposes Internal R&D Short-term use 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Our business partners Professional services organizations Government entities
Inferences drawn from any of the information identified above	<ul style="list-style-type: none"> You Your Use of Our Sites Affiliates, Subsidiaries or Vendors 	<ul style="list-style-type: none"> Performing the Services Auditing Quality Purposes and Safety Security Purposes Internal R&D Short-term use 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Professional services organizations Government entities
Sensitive Personal Information: including social security, driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; biometric information processed to identify you, or precise geolocation.	<ul style="list-style-type: none"> You Your Use of Our Sites Affiliates, Subsidiaries or Vendors 	<ul style="list-style-type: none"> Performing the Services Auditing Quality Purposes and Safety Security Purposes Internal R&D Short-term use 	<ul style="list-style-type: none"> Our affiliates and subsidiaries Service providers Professional services organizations, Government entities

Categories of Sources Explained: in the 12 months prior to the effective date of the Notice, Convera may have collected Personal Information about you from the following Categories of Sources:

- You:** we may collect information directly from you, for example, through your account, transaction forms and your interactions with Convera partners or through providing customer support or consultation, including using email, postal mail, call centers or live chat;
- Your Use of Our Sites:** we may collect information from you or your device through your use of our Sites, including online forms, registrations for loyalty and rewards programs or competitions, and other online Services or applications we offer (some of which may be managed by third parties on behalf of Convera) or through automated means such as communications protocols, email communications and cookies or similar technologies as described in the Global Privacy Notice section titled "[Internet Technologies](#)";

- **Affiliates, Subsidiaries or Vendors:** we may collect information about you from our affiliates, subsidiaries or vendors who provide services on our behalf;
- **Third parties:** we may collect information from other sources such as banks, financial institutions, commercial sources, or law enforcement bodies;
- **Social Media Networks or Publicly Available Sources:** we may collect information about you from social media or other public data sources; and
- **Advertising Networks:** we may collect information about you from advertising networks so we can serve you with advertisements we believe may be of interest to you.

Business Purposes Explained: in the 12 months prior to the effective date of the Notice, Convera may have shared your Personal Information for the following Business Purposes:

- **Auditing:** related to our interactions with you and any concurrent transactions, including, but not limited to, counting ad impressions, verifying positioning and quality of ad impressions, and auditing compliance with applicable standards;
- **Security Purposes:** detecting security incidents, protecting against malicious, deceptive, fraudulent or illegal activity and prosecuting those responsible for that activity;
- **Debugging:** debugging to identify and repair errors that impair the intended functionality of our systems;
- **Short-term use:** short term, transient use, including, but not limited to, the contextual customization of ads shown as part of your interactions with us;
- **Performing the Services:** in addition to the purposes described in the Global Privacy Notice, maintaining or servicing accounts, identifying and authenticating you, providing customer service, processing or fulfilling orders and transactions, verifying your information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services;
- **Internal R&D:** undertaking internal research for technological development and demonstration; and
- **Quality Purposes:** undertaking activities to verify or maintain the quality or safety of the Services and to improve, upgrade or enhance the Services.

Categories of Third Parties Explained: in the 12 months prior to the effective date of the Notice, Convera may have shared your Personal Information with the following Categories of Third Parties:

- **Our affiliates and subsidiaries;**
- **Service providers:** relating to hosting and internet services, business and communication tools, Customer Relationship Management (CRM), document management, payment processes, identity verification, payments and fraud risk management, and marketing;
- **Our business partners:** who facilitate our payment transactions or provide specific Services you have requested;
- **Professional services organizations:** such as law firms and independent auditors;
- **Data analytics providers;**
- **Operating systems and platforms;**
- **Advertising and social networks:** advertising and social networks (who may combine your Personal Information with their own records, and records available from other sources for their own marketing purposes); and
- **Government entities:** government entities including law enforcement agencies;

U.S. State Privacy Rights

U.S. State residents may have certain rights relating to their personal information. Note that these rights only apply to Personal Information we process in our capacity as an entity that determines the purposes and means of processing (i.e., as a business or controller). If your relationship with us is through one of our business clients, you must submit your privacy rights request directly to the client with whom you have a primary relationship.

In general, you may have the following rights, subject to certain exceptions:

- **The right to opt-out of the Sale of Your Personal Information**

Some U.S. State Privacy Laws provide you with the right to opt out of the “sale” of your Personal Information. Convera does not sell Personal Information to third parties in exchange for money. However, because “sale,” as used under these U.S. State Privacy Laws, is broadly interpreted to include the use of third-party advertising, marketing, and analytics cookies, and “sharing” to include disclosure of Personal Information for cross-context behavioral advertising purposes, we may be considered “selling” and “sharing” Personal Information simply because our Sites may use such cookies or similar technologies. This is the only use case where Convera may be considered to “sell” or “share” Personal Information under U.S. State Privacy Laws.

In light of the above, for the 12 months prior to the effective date of the Notice, Convera may have “sold” or “shared” the following categories of Personal Information:

- Identifiers: contact information, for example your name, email address and telephone number; and
- Internet and Other Electronic Network Activity Information: including the host from which you access the Internet, your IP address or device advertising ID, information about your device (such as device properties, settings, applications, storage and usage information), mobile application, browser and operating system software, social profile and network information, the date and time you access our websites and the address of the site from which you linked to our website when you visit us.

To exercise your right to opt-out, please use our cookie preferences center available at <https://convera.com/compliance-legal/cookie-policy/>. You also have the right to opt-out of “sales” and “sharing” of your personal information using an opt-out preference signal. If our site detects that your browser or device is transmitting an opt-out preference signal, such as the “global privacy control”—or GPC— signal, we will opt that browser or device out of the use of cookies or other tools on our site that result in a “sale” or “sharing” of your Personal Information. If you come to our site from a different device or from a different browser on the same device, or if you clear your cookies, you will need to opt-out again, or use an opt-out preference signal, for that browser and/or device as well.

Convera does not sell or share Personal Information of individuals we know are under 16 years of age.

- **The right to opt-out of the processing of your Personal information for certain advertising purposes**

Some U.S. State Privacy Laws provide you with the right to opt out of the processing of your Personal Information for purposes of serving you advertisements that are relevant to you based on your activity across our services and other sites (“targeted advertising” or “cross-contextual behavioral advertising”), including the sharing of your Personal Information for these targeted advertising purposes. Convera may use services that help deliver interest-based ads to you, and our Sites may use third-party cookies or similar technologies that collect your Personal Information. You can exercise your right to opt-out via our Privacy Preference Centre or visit the Cookie Policy link in the footer of our Site. Please note that some transfers of your Personal Information may not be for purposes of targeted advertising, and certain exemptions may apply under applicable U.S. State Privacy Laws.

- **The right to limit use of Sensitive Personal Information**

You have the right to ask us to limit our use of your Sensitive Personal Information to certain purposes. However, we do not engage in uses or disclosures of sensitive Personal Information that would trigger this right under the U.S. State Privacy laws.

- **Access, correct, opt-out, delete and appeal rights**

- Right to Know/Access: You have the right to request a copy of the specific pieces of Personal Information we have collected about you, and certain information about our processing activities that may be available to you in this Privacy Notice. Please note that some State Privacy Laws may prohibit businesses from including certain elements of Sensitive Personal Information, such as payment card number, in their access reports, even if you have provided those data elements.
- Right to Correct: You have the right to request we correct incorrect Personal Information. In certain circumstances we may also delete the contested Personal Information rather than correcting it if it does not negatively impact you or if you consent to deletion as an alternative to correction.
- Right to Delete: You have the right to request we delete your Personal Information. If you request that we delete your Personal Information, we will do so except in those situations where our retention is permitted by the applicable U.S. State Privacy Laws (such as for fraud prevention or legal compliance, or where reasonably necessary to provide the services requested or for our internal business purposes). In these situations, we will retain your information in accordance with our records retention program and securely delete it at the end of the retention period.
- Right to Opt-out: You have the right to opt-out of automated decisions that involve your Personal Information and have legal or similarly significant effects.
- Right to Non-Discrimination: We will not discriminate against you in terms of price or service level for exercising any of your privacy rights.

You may exercise your rights, authorize another person to act on your behalf, or appeal a denial of a request by:

- emailing us at privacymatters@convera.com or contacting us as indicated on our website <https://convera.com/>
- submitting a request via the Convera [Privacy webform](#)
- mailing us a letter at: Convera USA, LLC, Privacy Office, 7979 E. Tufts Avenue, Suite 200, Denver, CO 80237, USA

Before responding to your request we must verify your identity. Please provide your full name, the email address you use to interact with us, and your address or phone number if you have provided this to us. We will take steps to verify your request by matching the information provided by you with the information we have in our records. In some cases, we may request additional information in order to verify your identity, or where necessary to process your request. If we are unable to verify your identity after a good faith attempt, we may deny the request and, if so, will explain the basis for the denial.

Convera cannot connect individual consumers to passive website visits which may affect our ability to respond to certain requests. Convera has implemented the capability for the user to manage cookies on our websites and will only read or write cookies based on your preference level. When you visit our website, you will be presented with a banner instructing you how to manage your preferences.

You may also designate an authorized agent to make a Personal Information request on your behalf. If you choose to designate an agent, we may require the authorized agent to provide us with evidence of your written permission to make your request and may ask you to verify your own identity directly with us. For your security, we may deny a request from an agent that does not submit proof that they have been authorized by you to act on your behalf.

- **Additional disclosures for large businesses**

The CCPA requires certain businesses to compile and disclose information each year regarding their compliance with the CCPA for the previous twelve-month period. Convera does not qualify as a large data collector under CCPA.

- **Accessibility**

If you need this information in an alternative accessible format, you may contact us as indicated above.

Appendix I – Convera Legal Entities

COUNTRY	ENTITY	DATA PROTECTION AUTHORITY
Australia	Convera Australia Pty Ltd Level 12 1 Margaret Street , Sydney NSW, New South Wales, 2000 Australia	Office of the Australian Information Commissioner (OAIC) (www.oaic.gov.au/)
Canada	Convera Canada ULC 1500-100 Yonge Street, Toronto, Ontario, M5C2W1, Canada	Office of the Privacy Commission of Canada (OPC) (www.priv.gc.ca/en/)
Hong Kong	Convera Hong Kong Ltd Unit 2210-18, Tower 1, Millennium City 1, 388 Kwun Tong Road, Kwun Tong, Kowloon, Hong Kong	Office of the Privacy Information Commissioner, Hong-Kong (PDPC) (https://www.pcpd.org.hk/)
Japan	Convera Japan KK c/o Kusunoki, Iwasaki & Sawano, Holland Hills Mori Tower 11F 5-11-1, Toranomon, Minato-ku, Tokyo 105-0001, Japan	Personal Information Protection Commission (PPC) (www.ppc.go.jp/en/index.html)
Luxembourg	Convera Europe Financial S.A. OBH Building, 6b rue du Fort Niedergrunewald, L-2226 Luxembourg Convera Europe S.A OBH Building, 6b rue du Fort Niedergrunewald, L-2226 Luxembourg	National Data Protection Commission – Luxembourg (CNPd) (https://cnpd.public.lu/en.html)
Malta	Convera Malta Financial Limited W Business Centre, Level 5, Triq Dun Karm, Birkirkara By-Pass, Birkirkara, BKR 9033, Malta	Information and Data Protection Commissioner (IDPC) (https://idpc.org.mt/)
Singapore	Convera Singapore Financial Pte Ltd 77 Robinson Road, #35-01 Robinson 77 Singapore, 068896 Convera Singapore Pte Ltd 77 Robinson Road, #35-01 Robinson 77 Singapore, 068896	Personal Data Protection Commission (PDPC) (www.pdpc.gov.sg/)
Switzerland	Convera Switzerland Limited, London (UK), Zurich Branch Werdstrasse 2, P.O. Box 2063, 8021 Zurich, Switzerland	Federal Data Protection and Information Commissioner (FDPIC) (https://www.edoeb.admin.ch/en)
United Kingdom	Convera UK Financial Limited Alphabeta Building, 3 rd Floor, 14-18 Finsbury Square, London, EC2A 1AH, United Kingdom Convera UK Limited Alphabeta Building, 3 rd Floor, 14-18 Finsbury Square, London, EC2A 1AH, United Kingdom	Information Commissioner's Office (ICO) (www.ico.org.uk)
United States	Convera USA, LLC The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street Mailing address: 7979 E. Tufts Avenue, Suite 400 Denver, CO 80237	