

PayQuicker, LLC Privacy Policy

In this Policy, the terms “PayQuicker,” “we,” “us” or “our” shall refer to PayQuicker LLC. The terms “you”, “your” shall refer to any individual or entity who accepts this Policy.

Effective date: March 15, 2025

This privacy policy (“Policy”) has been compiled to better serve those who are concerned with how their Personal Data is being used by us. This Policy is to inform you of our policies and procedures regarding the collection, use and disclosure of Personal Data we receive from users of our website (www.payquicker.com) and services, including but not limited to our platform, product, or accounts (individually and collectively, the “Services”). This Policy applies only to information that you provide to us through the Services. This Policy does not apply to information you provide to any third-party service provider(s) related to or whose services are incorporated into or provided by the Services (“Third Parties”); information you provide to Third Parties shall be controlled by their respective privacy policies. The Services may be provided to you pursuant to additional terms and conditions. For example, you may have an Account services agreement for an Account, and the Services are further subject to the Terms of Service. Capitalized terms not defined in this Policy shall have the meaning ascribed to them in such additional agreements.

Please read our Policy carefully to get a clear understanding of how we collect, use, protect or otherwise handle your Personal Data in accordance with the Services.

Legal Basis for Processing

We process your Personal Data pursuant to contractual necessity to carry out the Services for you, and further pursuant to your consent. Your use of the PayQuicker Services constitutes your acceptance and consent to be bound by this Policy. If you do not agree with any of the terms of the Privacy Policy, you do not have the right to access or otherwise use the Applications or Services. Note that PayQuicker supports the right to withdraw consent for those consumers granted that right in their jurisdiction, but upon the withdrawal of consent various services (possibly all) will become unavailable, depending on the scope of the withdrawn consent.

What Personal Data do we collect from you?

Personal Data is personal information that can be associated with an identified or identifiable person. “Personal Data” can include name, postal address, telephone number, email address, other financial account information, account number, date of birth, and government-issued credentials (e.g., driver’s license number). Personal Data does not include information that does not identify a specific User.

We collect Personal Data when you visit our website or utilize our Services, including the following:

Registration and use information: we collect Personal Data when you apply for a PayQuicker account or if you otherwise use our platform, website, or phone application to send or receive funds. This registration and use information may include:

- *Consumer Identity Information* – your name or aliases, physical address, phone number, email address, date of birth, gender, social security number or other tax identification number, photo identification, selfie, or video authorization, or any other information you choose to provide.

- *Business Identity Information* – entity legal name or aliases / “doing business as” names, physical address, phone number, entity type, industry, organizational documents (e.g. articles of incorporation), employer identification number, or other information relating to your authorized signors or beneficial owners.

Transaction Information: As you use your PayQuicker account, or otherwise send or receive funds through our or our Corporate Clients and Partners websites or applications, we collect Personal Data in connection with each transaction, including transaction time, transaction amount and currency, and details relating to the sender or receiver of funds. We may also collect receipts, contracts, photos, memos or other information relating to your transactions.

Corporate Client and Partner Information: When you communicate with us or our Corporate Client and Partners about the Services, we may collect information related to said communication, including but not limited to, device and account information, as well as the contents within the communication .

Customer Support: Information you provide to our customer support may be collected in order to provide services or assistance requested by you.

Digital identity information: Your access to the Services is primarily limited to your internet connected devices. As a result, we may collect some Personal Data relating to your digital identity such as that includes an IP address, your device “fingerprint” (e.g. hardware model, operating system and version, unique device identifiers and mobile network information), browser type, and pages visited on our website.

Third party sources: When you create a PayQuicker Account or otherwise send or receive funds through PayQuicker or our Corporate Client’s and Partner’s websites or phone applications, we may collect information, including Personal Data, about you from non-affiliated third party service providers in order to verify your identity and to prevent fraud, and provide our Services to you, including information relating to your location, phone number, email address, and prior addresses and names.

Publicly shared information: Additionally, we may collect information you share publicly on your social media accounts. If you do not wish to share this information publicly on your social media accounts, you should adjust your privacy settings with the site.

While not all the Personal Data described above is necessary to use our Services, if you opt out of sharing some of this information, this may affect your ability to use your PayQuicker account or other services offered by us or our Corporate Clients and Partners.

If you choose not to give personal information

If you choose not to give us your personal information, it may mean that we cannot perform the services needed to run your account. It could mean that we cancel your account or services you have with us.

How do we use Cookies and tracking technology?

If you visit our website, we use various technologies to collect information on our services and other websites, and this may include sending cookies to your computer or mobile device. Cookies are small data files stored on your hard drive or in device memory that help us improve our services and your experience, see which areas and features of our services are popular and count visits. While most web browsers are set to accept cookies by

default, if you prefer, you can usually choose to set your browser to remove or reject browser cookies. Please note that if you choose to remove or reject cookies, this could affect the availability and functionality of our website or other services. You can read more about our use of cookies at our Cookie Policy:

<https://payquicker.com/cookie-policy/>.

We may also collect information using web beacons (also known as “tracking pixels”). Web beacons are electronic images that may be used in our Services or emails and help deliver cookies, count visits, understand usage, mitigate fraud, and determine whether an email has been opened and acted upon.

We honor Do Not Track signals and we do not track, plant cookies, or use advertising when a Do Not Track (DNT) browser mechanism is in place.

How do we use your information?

Data retention

We retain Personal Data to fulfill our legal or regulatory obligations and for our business purposes. We may retain Personal Data for longer periods than required by law if it is in our legitimate business interests and not prohibited by law. If your Account is closed, we may take steps to mask Personal Data and other information, but we reserve our ability to retain and access the data for so long as required to comply with applicable laws. We will continue to use and disclose such Personal Data in accordance with this Privacy Policy.

Processing of Personal Data

We may act in different roles, either as a data controller or data processor, when processing your Personal Data. In general, a data controller is the person or entity that alone or jointly determines the purposes and means for processing data, and a data processor performs actions with data to carry out a data controller’s instructions. In some instances we will be the data controller and in others, we may be the data processor. For example, when we use your Personal Data to perform Services initiated by you or a Corporate Client, we are a data processor. But, for example, if we use Personal Data to market Services to you, we are the data controller.

Process or Processing of data means any method or way that we handle Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, and consultation, disclosure by transmission, disseminating or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data.

We process Personal Data for the following reasons:

- Provide, maintain and improve the PayQuicker Account services, and other Services we offer you with our Corporate Clients and Partners;
- Provide and deliver the products and services you request or opt in to, process transactions and send you related information, including confirmations;
- Verify your identity and prevent fraud;
- Communicate between our Corporate Clients and Partners (as applicable) in order to provide Services to you;
- Send you technical notices, updates, security alerts and support and administrative messages;
- Respond to your comments, questions and requests and provide customer service;
- Monitor and analyze trends, usage and activities in connection with our Services;

- Personalize and improve the Services based on your usage;
- Link or combine with information we get from others to help understand your needs and provide you with better service; and
- For user authentication determination, fraud mitigation and security assessment and determination, and location determination to provide location-based services.

How do we share your Personal Data?

We may disclose any information we collect about current and former customers, including Personal Data, to affiliates and non-affiliated third parties as follows:

- With financial institutions and financial services providers, including the Partner that provides banking services in connection with your PayQuicker account;
- With the Corporate Client identified in your PayQuicker account agreement that provides payment and other services to you in connection with your PayQuicker account;
- With non-financial companies, such as identity verification service providers and fraud prevention service providers that use the information to provide services to PayQuicker and other companies; and
- With other non-affiliated companies for our everyday business purposes, such as to process transactions, maintain accounts, respond to court orders and legal investigations, report to credit bureaus, or provide services that you have opted in to. For example, in connection with our everyday business purposes, we may share information about you in cases that include but are not limited to the following scenarios:
 - In response to a request for information, if we are required by, or we believe disclosure is in accordance with, any applicable law, regulation or legal process;
 - With relevant law enforcement officials or other third parties, such as investigators or auditors, if we believe it is appropriate to investigate fraud;
 - If we believe your actions are inconsistent with the spirit or language of our user agreements or policies, or to protect the rights, property and safety of PayQuicker or others;
 - In connection with, or during negotiations of, any merger, sale of PayQuicker's assets, financing or acquisition of all or a portion of our business to another company; and
 - At your direction.

Aggregated Data: We may also share aggregated or de-identified Information, which cannot reasonably be used to identify you and which does not include Personal Data. For example, we may share certain transaction details such as amounts and zip codes in a pseudo-anonymous fashion to promote security and validity of PayQuicker's services.

Financial crime prevention: We will use your personal information to help decide if your accounts may be being used for fraud or money-laundering. We may detect that an account is being used in ways that fraudsters work, or we may notice that an account is being used in a way that is unusual. If we think there is a risk of fraud, we may stop activity on the accounts or refuse access to them. We might also check and share your information with fraud prevention agencies. If fraud is identified or suspected, these agencies may keep a record of that information and we may refuse to provide any services. Law enforcement agencies may access and use this information.

How do we protect your information?

We take commercially reasonable measures to help protect your Personal Data from loss, theft, misuse and unauthorized access, disclosure, alteration, and destruction. Additionally, we implement policies designed to protect the confidentiality and security of your Personal Data. Except as detailed herein and as it relates to our Corporate Clients and Partners, we limit access to your Personal Data to employees that have a business reason to know such information and implement security practices and procedures designed to protect the confidentiality and security of such information and prohibit unlawful disclosure of such information in accordance with our policies.

Additionally:

- Our website is scanned on a regular basis for security holes and known vulnerabilities in order to make your visit to our site as safe as possible.
- We regularly scan for malware and verify the security of our servers.
- All sensitive information (e.g., personal data, credit / transaction data) you supply is encrypted via Secure Socket Layer / Transport Layer Security (SSL/TLS) technology.
- We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your information.
- All transactions are processed through a gateway provider and are not stored or processed on our servers.

While we deploy the above mechanisms, the transmission of information via the internet is not completely secure. The safety and security of your information also depends on you taking appropriate precautions to protect yourself while on the internet and we do not guarantee or warrant the security of your Personal Data transmitted to our website or in connection with the Services. Any transmission of Personal Information is at your own risk and we are not responsible for your circumvention of any privacy settings or security measures contained on the website.

Children's Privacy

We comply with the U.S. Children's Online Privacy Protection Act and the regulations implementing it ("COPPA"), to the extent applicable to us and to PayQuicker Services. We do not knowingly collect "personal information," as defined under COPPA, directly from users under the age of 13. If you are under 13, do not use or provide any information through the PayQuicker Services or through any of its features. If we learn we have collected or received personal information from a child under 13 without verification of parental consent, we will delete that information. If you believe we might have any information from or about a child under 13, please contact us as described below in *"How to Contact Us"*.

Changes To and Scope Of Our Policy

We may, in our sole and absolute discretion, change or modify this Policy, and any policies or agreements which are incorporated herein, at any time, and such changes or modifications shall be effective immediately upon posting to the website. No revision or update will apply to a dispute which we had actual notice of on the date we posted the changes or modifications. We will notify you of such changes or modifications by posting them to the website or direct communication with you, and your use of the Services after such changes or modifications

have been posted (as indicated by the “*Effective Date*”) shall constitute your acceptance of the Policy as last revised. If you do not agree with the Policy as last revised, do not use (or continue to use) the Services.

Choice Relating To Your Personal Data

Personal Data: You may have the ability review, update, correct or delete all or some of the Personal Data in your PayQuicker account by contacting us or by editing your profile via the website. If you completely delete all such information, then your PayQuicker account may become deactivated. We may retain an archived copy of your records as required by law or for legitimate business purposes.

Location and other device-level information: The device you use to access the Services may collect information about you, including geolocation information and usage data that PayQuicker may then collect and use. For information about your ability to restrict the collection and use of such information, please use the settings available in the device.

Marketing Communication Notices: We may send you marketing content about our Applications and Services, through various communication channels, for example, email, text, pop-ups, push notifications, and messaging applications. You may opt out of these marketing communications by following the instructions in the communications you receive. If you have an Account with us, you may also be able to adjust your communication preferences in your Account settings. For messages sent via push notifications, you may manage your preferences in your device.

Does our site allow third-party behavioral tracking?

It's also important to note that we allow our services providers to use behavioral tracking for purposes of security and fraud prevention in connection with providing the Services. These service providers are required to only utilize the information for purposes of providing the Services.

Third Party Links

Occasionally, at our discretion, we may include or offer third party products or services on our website. These third-party sites have separate and independent privacy policies. We therefore have no responsibility or liability for the content and activities of these linked sites. Nonetheless, we seek to protect the integrity of our site and welcome any feedback about these sites.

International Data Transfers

Our operations are supported by a network of computers, cloud-based servers, and other infrastructure and information technology, including, but not limited to, third-party service providers. We and our third-party service providers store and Process your Personal Data in the United States and elsewhere in the world, and in accordance with applicable privacy law. This means that your Personal Data may be transferred outside your country of origin for processing, predominantly to the United States, but also to the host countries of our partners in some cases. Any data being processed within a given country may be accessed by the courts, law enforcement, and/or national security authorities of the country where it is being processed, following the applicable laws of that country.

In connection with the transfer of your Personal Data outside the European Union, we will make such transfer in accord with applicable privacy law, and when applicable, in accord with the contractual, technical, and organizational measures via contractual agreement with such third party.

Supplemental Notice for EEA, UK, and Switzerland

If you are located in the European Economic Area (“EEA”), the UK or Switzerland, we comply with applicable laws to provide an adequate level of data protection for the transfer of your Personal Data to the US. PayQuicker complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. PayQuicker has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. PayQuicker has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>. With respect to personal data received or transferred pursuant to the Data Privacy Frameworks, PayQuicker is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). See the [Data Privacy Framework Policy](#) for details.

By using our Applications and Services, you consent to your Personal Data being transferred to other countries, including countries that have different data protection rules than your country. We do not represent that our Applications and Services are appropriate or available in any particular jurisdiction.

Your Rights

These privacy regulations give certain rights to individuals in relation to their personal data. If any of these privacy regulations apply to you or your Personal Data, you have certain rights with respect to that data. These rights include:

- **Right of Access.** You have the right to be informed of and request access to the personal data we process about you.
- **Right to Rectification.** You have the right to request that we amend or update your personal data where it is inaccurate or incomplete.
- **Right to Erasure.** You have the right to request that we delete your personal data.
- **Right to Restrict.** You have the right to request that we temporarily or permanently stop processing all or some of your personal data.
- **Right to Object.** You have the right, at any time, to object to us processing your personal data on grounds relating to your particular situation. You have the right to object to your personal data being processed for direct marketing purposes.
- **Right to Data Portability.** You have the right to request a copy of your personal data in electronic format and the right to transmit that personal data for use in another party’s service.
- **Right not to be subject to Automated Decision-making.** You have the right to not be subject to a decision based solely on automated decision making, including profiling, where the decision would have a legal effect on you or produce a similarly significant effect.

If you or your authorized agent wishes to exercise any of these rights, please contact us as outlined in the “*How to Contact Us*” section below. Further, if the GDPR is applicable to you or your Personal Data and you are unhappy with how we are using your Personal data, you can also contact and file a complaint with your local Data Protection Authority.

You may also have the right to make a GDPR complaint to the relevant Supervisory Authority. A list of Supervisory Authorities is available here: https://edpb.europa.eu/about-edpb/about-edpb/members_en. If you need further assistance regarding your rights, please contact us using the contact information provided below and we will consider your request in accordance with applicable law. In some cases, our ability to uphold these rights for you may depend upon our obligations to process personal information for security, safety, fraud prevention reasons, compliance with regulatory or legal requirements, or because processing is necessary to deliver the services you have requested. Where this is the case, we will inform you of specific details in response to your request.

Supplemental Notice for Canadian Consumers

This section provides additional details about the personal information we collect about Canadian consumers and the rights afforded to them under various laws. If you or your authorized agent wishes to exercise any of these rights, please contact us as outlined in the “*How to Contact Us*” section below. If unsatisfied with any PayQuicker remediation related to privacy rights, Canadian consumers can escalate their complaints to Privacy Commissioner of Canada here: <https://www.priv.gc.ca/en>.

PIPEDA – All Canadian Consumers

Personal data, as defined in the Personal Information Protection and Electronic Documents Act (“PIPEDA”) will be collected, stored, used, and/or processed by PayQuicker in accordance with PayQuicker’s obligations under PIPEDA.

Quebec Law 25 – Quebec Consumers

Subject rights under Law 25 resemble those found under the EU General Data Protection Regulation (GDPR) noted above. Subject rights in Quebec now include:

- **Right to be informed.** You have the right to be informed of any collection of your personal data, the purpose for each collection, and the method of collection, and consent to any or all of this data collection / use.
- **Right to access.** You have the right to be informed of and request access to the personal data we process about you.
- **Right to rectification.** You have the right to request that we amend or update your personal data where it is inaccurate or incomplete.
- **Right to erasure.** You have the right to request that we delete your personal data.
- **Right to withdraw consent.** You have the right to withdraw any previously issued consent.
- **Right to restrict processing.** You have the right to request that we temporarily or permanently stop processing all or some of your personal data.
- **Right to data portability.** You have the right to request a copy of your personal data in electronic format and the right to transmit that personal data for use in another party’s service.

Supplemental Notice for California Consumers

This section provides additional details about the personal information we collect about California consumers and the rights afforded to them under the California Online Privacy Protection Act (CalOPPA) and the California Consumer Privacy Act (CCPA), as amended and extended by the California Privacy Rights Act (CPRA).

California Online Privacy Protection Act (CalOPPA)

CalOPPA is the first state law in the nation to require commercial websites and online services to post a privacy policy. The law's reach stretches well beyond California to require any person or company in the United States (and conceivably the world) that operates websites collecting Personally Identifiable Information from California consumers to post a conspicuous privacy policy on its website stating exactly the information being collected and those individuals or companies with whom it is being shared. See more here: <http://consumercal.org/california-online-privacy-protection-act-caloppa/#sthash.0FdRbT51.dpuf>.

According to CalOPPA, we agree to the following:

- Once this Policy is created, we will add a link to it on our home page or as a minimum, on the first significant page after entering our website.
- Our Policy link includes the word 'Privacy' and can easily be found on the page specified above.

Your Rights under CPRA/CCPA

Subject to applicable law, you have the following rights with respect to your personal information.

- **Right to access.** You have the right to request that we disclose to you what personal information we collect, use, disclose, share, and sell about you.
- **Right to delete.** You have the right to request that we delete your personal information that we've collected.
- **Right to update.** You have the right to request that inaccurate personal information we hold about you be corrected.
- **Right to restrict the use and disclosure of your sensitive information.** You have the right to request that we limit our use and disclosure of your sensitive personal information.
- **Right to nondiscrimination.** You have the right not to receive discriminatory treatment because you've exercised any of your rights under the CPRA.

If you or your authorized agent wishes to exercise any of these rights, please contact us as outlined in the *"How to Contact Us"* section below.

No Sale or Sharing of Personal Information

As defined under CPRA/CCPA, we do not sell or share your personal information. Rather we only disclose your Personal Data as are necessary for us to provide products or services to you (as you have agreed to or opted in to) and for our authorized business purposes.

Limitations

PayQuicker strives to protect your information and data; however, some privacy issues may be unintentionally missed, so PayQuicker cannot guarantee error-free performance. PayQuicker is not responsible for any damages, including incidental, consequential, or punitive damages, relating to the practices described in this Privacy Policy.

English Language Controls

Translations of this Agreement that may have been provided are for your convenience only and may not accurately reflect the original English meaning. The meanings of terms, conditions, and representations herein are subject to definitions and interpretations in the English language.

How to Contact Us

If there are any questions regarding this Policy, you may contact the Privacy Officer and Data Protection Officer using the information below. Please note that we may ask you or your agent to provide us with additional information to confirm your identity.

Email: dpa@payquicker.com

Mail:

PayQuicker, LLC
ATTN: Privacy and Data Protection Officer
400 Linden Oaks, Suite 320
Rochester, New York 14625
USA