Privacy Policy

Created: January 2, 2021
Reviewed/Updated: July 15, 2025

OUR COMMITMENT TO PRIVACY

Spendr Inc. ("Spendr") knows that you care about how your personal information is used and shared, and we take your privacy seriously. Our primary goal is to provide you with exceptional service, and we understand that you may have questions or concerns regarding your personal information and how it will be used. To make this privacy policy easy to find, we make it available from the home page of the Spendr website at www.spendr.com (the "website") and through our mobile applications. You may also email us at support@spendr.com with any privacy-related questions you have.

APPLICABILITY OF PRIVACY POLICY

This privacy policy applies to all information we collect from current and former Spendr users in connection with the Services, including you. "Services" means any products, services, content, features, technologies, or functions, and all related websites, applications and services offered to you in connection with a Spendr Wallet Account. When you are no longer our customer, we continue to share your information as described in this policy.

Throughout this policy, we use the term "personal information" to describe information that can be associated with a specific person and can be used to identify that person. We do not consider personal information to include information that has been aggregated and/or anonymized so that it does not identify a specific user. All terms not otherwise defined herein have the same meanings ascribed to such terms under the Spendr Inc. Terms and Conditions of Service ("Terms and Conditions").

THE INFORMATION WE COLLECT

When you visit the website or use our mobile application or other Services, we collect your IP address, and standard web log information, such as your browser type and the pages you accessed on our website. We also may collect Geolocation Information (defined below). If you do not agree to our collection of this information, you may not be able to use our Service.

If you open a Spendr Digital Wallet Account, we collect the following information from you:

Wallet Account Information – text-enabled cellular/wireless telephone number, machine or mobile device ID and other similar information.

Identification Information – your name, street address, email address, date of birth, and Driver's License or Passport information (if necessary to fulfil KYC requirements).

Device Information – information about you: (a) from your mobile device or computer such as your device type, machine or mobile device identification number, Geolocation Information, time zone, language setting, browser type, and IP address, and (b) from third parties for purposes of transaction processing, identity verification, fraud detection or prevention and other similar purposes. For fraud prevention purposes, we also may link your machine ID with the machines of others who use your same payment cards.

Geolocation Information – information that identifies with reasonable specificity your location by using, for instance, longitude and latitude coordinates obtained through GPS, Wi-Fi, or cell site triangulation. We will collect this data for fraud and risk purposes. In addition, some of our Services may ask you for permission to share your current location within your device settings to enhance our Services. If you do not agree to our collection of Geolocation Information, our Services may not function properly when you try to use them. For information about your ability to restrict the collection and use of Geolocation Information to enhance our Services, please refer to the settings available in your device.

Financial Information – bank account online login information, Designated Bank Account and routing numbers linked to your Spendr Wallet Account, and Designated Bank Account balance information (only when Wallet loads occur).

We are committed to providing a safe, secure and all-around great service. Therefore, before permitting you to use the Services, we may require additional information from you we can use to verify your identity, address or other information or to manage risk and compliance throughout our relationship. We may also obtain information about you from third parties, including, but not necessarily limited to, credit reporting agencies, such as identity verification, fraud prevention and similar services.

When you are using the Services, we collect information about your Wallet Account transactions, and we may collect Geolocation Information and/or information about your computer or other access device for fraud prevention and other similar purposes.

Finally, we may collect additional information from or about you in other ways not specifically described here. For example, we may collect information related to your contact with our customer support team or store results when you respond to a survey.

HOW WE USE COOKIES

When you visit or use our web site, we and certain business partners and vendors may use cookies and other tracking technologies (collectively, "Cookies"). We use Cookies to recognize you as a customer; customize Services, other content and advertising; measure the effectiveness of promotions; perform a wide range of analytics; mitigate risk and prevent potential fraud; and to promote trust and safety across our Services.

Certain Services are only available through the use of Cookies, so if you choose to disable or decline Cookies, your use of certain Services may be limited or not possible.

Do Not Track: Do Not Track ("DNT") is an optional browser setting that allows you to express your preferences regarding tracking by advertisers and other third-parties. We do not respond to DNT signals.

HOW WE PROTECT & STORE PERSONAL INFORMATION

We store and process your personal information using third party servers located in data centers in the United States. Consistent with the requirements of the Gramm Leach Bliley Act, we have implemented administrative, technical, and physical safeguards designed to:

Ensure the security and confidentiality of customer information, including nonpublic personal information.

Protect against any anticipated threats or hazards to the security of such information; and

Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

We also use computer safeguards such as firewalls, 2FA and data encryption, we enforce physical access controls to our office and files, and we authorize access to personal information only for those employees who require it to fulfill their job responsibilities.

We strive to ensure security on our systems. Despite our efforts, we cannot guarantee that personal information may not be accessed, disclosed, altered or destroyed by breach of our administrative, managerial and technical safeguards. Therefore, we urge you to take adequate precautions to protect your personal data as well, including never sharing your Spendr password with anyone.

If Spendr learns of a systems security breach, we may attempt to notify you electronically so that you can take appropriate protective steps. By using the Services, you agree that Spendr may communicate with you electronically. Spendr may post a notice on the website or mobile application if a security breach occurs. We may also send an email to you at the email address you have provided to us. Depending on where you live, you may have a legal right to receive notice of a security breach in writing. To receive free written notice of a security breach (or to withdraw your consent from receiving electronic notice of a security breach), please email us at support@spendr.com.

HOW WE USE THE PERSONAL INFORMATION WE COLLECT

Our primary purpose in collecting personal information is to provide you with a safe, smooth and efficient experience. We may use your personal information to:

Provide the services and customer support you request.

Process transactions and send notices about your transactions or your network activity.

Resolve disputes, collect fees, and troubleshoot problems.

Prevent potentially fraudulent, prohibited or illegal activities, and enforce our Terms and Conditions through the use of our risk and fraud tools which may include use of Account Information, Identification Information, Financial Information, Device Information and Geolocation Information.

Create an account connection between your Spendr Wallet Account and any applicable third-party account or platform, including but not limited to your Designated Bank Account.

Customize, personalize, measure, and improve our services and the content and layout of our website.

Send you updates about new products and services that we are offering to customers.

Compare information for accuracy and verify it with third parties.

Perform other duties as required by law; and

If you elect to share your Geolocation Information, we will use this information to enhance the security of the Services and we may use this information to provide you with location-specific options, functionality, offers, advertising, search results, or other location-specific content.

HOW WE SHARE PERSONAL INFORMATION WITHIN THE SPENDR NETWORK

To process payments on Spendr, we need to share some of your personal information with the Participating Merchant and its affiliated depository institution.

We work with Participating Merchants to enable them to accept payments from you using Spendr. In doing so, a Participating Merchant may share information about you with us, such as your mobile phone number or Spendr username and Access Code, when you attempt to pay that Participating Merchant. We use this information to confirm to Participating Merchant that you are a Spendr customer and that the Participating Merchant should enable Spendr as a form of payment for your purchase.

Regardless, we will not disclose your Designated Bank Account information to any Participating Merchant, except with your express permission or if we are required to do so to comply with a subpoena or other legal process.

HOW WE SHARE PERSONAL INFORMATION WITH OTHER PARTIES

Spendr does not share your personal information with third parties for their promotional or marketing purposes.

Some personal information is public information and may be seen by anyone on the internet, regardless of any association with Spendr Certain public information may also be seen, accessed, reshared or downloaded through Spendr's APIs or third-party services that integrate with our products. Public information for personal profiles includes your Spendr username.

We may share your personal information with:

Our vendors and affiliates, but only for purposes allowed by this Policy.

Companies that Spendr plans to merge with or be acquired by or, in the event of any bankruptcy, a bankruptcy estate. Should such a combination occur, we will require that the new combined entity follow this privacy policy with respect to your personal information. If your personal information could be used contrary to this Policy, you will receive prior notice and the opportunity to communicate preferences you may have, if applicable.

Law enforcement, government officials, or other third parties if Spendr is compelled to do so by a subpoena, court order or similar legal procedure, when it is necessary to do so to comply with law, or where the disclosure of personal information is reasonably necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate violations of the Spendr Terms and Conditions, or as otherwise required by law.

Third party service providers who assist us in providing services to you, including, but not limited to, the Custodial Bank, or who provide fraud detection or similar services on our or any vendor's behalf.

Service providers under contract who help with parts of our business operations (for example, fraud prevention, payment processing, or technology services). Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own benefit.

Other third parties with your consent or at your direction to do so.

HOW YOU CAN ACCESS OR CHANGE YOUR PERSONAL INFORMATION

You can review and update your personal information in your account settings at any time by logging in to your account or by contacting Spendr Support at support@spendr.com or (513) 440-1590.

LINKS TO OTHER SERVICES OR SITES

The Services may contain links to (or allow you to link to) other third-party services or websites. Spendr does not control the information collection of third-party services or websites that can be reached through such links. We encourage our users to be aware when they are linking to a third-party service or website and to read the privacy statements of any third-party service or website that collects personally identifiable information.

RETENTION POLICY

Spendr will meet or exceed regulatory requirements for retention of records. Our standard is to retain all related customer, account and transaction data for as long as an account is active plus 7 years following deactivation.

CHANGES TO OUR PRIVACY POLICY

Spendr is always improving. As the Services evolve, we may occasionally update this privacy policy. If we modify this privacy policy, we will post the revised privacy policy to the website, and we will also revise the “last updated date” stated above. If we make material changes in the way we use personal information, we will notify you by posting an announcement on our mobile application or website or by sending you an e-mail. It is your responsibility to periodically review this privacy policy; users are bound by any changes to the privacy policy by using the Services after such changes have been first posted.

HOW TO CONTACT US

If you have questions or concerns regarding this privacy policy, or any feedback pertaining to your privacy and the Services that you would like us to consider, please email us at support@spendr.com or give us a call at (513) 440-1590.