Spendsafe

Privacy Policy

Table of Contents

1. Key Terms and Definitions

“Personal information” means information about an identifiable individual. It includes, without limitation, information relating to identity, nationality, age, gender, address, telephone number, email address, Social Insurance Number, date of birth, marital status, education, employment history, assets, liabilities, payment records, financial information, income and information relating to financial transactions as well as certain personal opinions or views of an Individual.

Personal information can also include information collected through Spendsafe’s website, such as device model, browser type and IP address. However, personal information does not include the name, title, business address or telephone number of a person or employee of an organization.

"Cardholder" means the individual who is registered as the prepaid cardholder. This is the individual approved for a Spendsafe prepaid card.

"Guardian" means the individual applying for the Spendsafe prepaid card on behalf of the cardholder. These are the parents, guardians, etc. associated with a client.

“Customers” means the cardholder and guardian collectively.

"**Database**" means the list of names, addresses, emails, telephone numbers, etc. of clients and guardians held by Spendsafe in the form of, but not limited to, computer files and files on computer hard-drives and that may be at least partly in the Software and/or the App.

“**Service Providers**” means the third-party company that Spendsafe procures services from (e.g. Peoples Trust Company and Onfido).

“**App**” means the app Spendsafe uses to carry on its business.

"**Express consent**" means the client or/and guardian has signed the application form, or other forms containing personal information, authorizing Spendsafe, and/or its Service Providers to collect, use, and disclose the individual's personal information for the purposes set out in the application forms, website or App, and this privacy manual.

"**Implied Consent**" means Spendsafe or its Service Providers may assume that the client or/and guardian consent to the information being used, retained and disclosed for the original purposes, unless notified by the client or/and guardian.

2. Policy Statement

2.1 Preamble

Spendsafe respects its customers' personal information and is committed to ensuring the proper use, disclosure, protection and security of all personal information placed under its care and in accordance with Schedule 1 of the personal Information Protection and Electronic Documents Act (PIPEDA).

Specifically, this privacy policy explains the personal information Spendsafe processes, how Spendsafe processes it, for what purposes and when to dispose of it. This policy should be read together with Spendsafe's AML/ATF Compliance Program manual.

Where there is a conflict, this policy will prevail. This policy applies to all Spendsafe's personnel (owners, senior management, employees) and Service Providers (data custodians, suppliers and contractors).

2.2 The Ten Principles of PIPEDA

The ten principles of PIPEDA that form the basis of this Privacy Policy are as follows:

1. **Accountability**: organizations are accountable for the personal information they collect, use, retain and disclose in the course of their commercial activities, including, but not limited to, the appointment of a Chief Privacy Officer;
2. **Identifying Purposes**: organizations are to explain the purposes for which the information is being used at the time of collection and can only be used for those purposes;
3. **Consent**: organizations must obtain an Individual's express or implied consent when they collect, use, or disclose the individual's personal information;
4. **Limiting Collection:** the collection of personal information must be limited to only the amount and type that is reasonably necessary for the identified purposes;
5. **Limiting Use, Disclosure and Retention**: Personal information must be used for only the identified purposes, and must not be disclosed to third parties unless the Individual consents to the alternative use or disclosure;
6. **Accuracy:** organizations are required to keep personal information in active files accurate and up-to-date;
7. **Safeguards**: organizations are to use physical, organizational, and technological safeguards to protect personal information from unauthorized access or disclosure.
8. **Openness**: organizations must inform their clients and train their employees about their privacy policies and procedures;
9. **Individual Access:** an individual has a right to access personal information held by an organization and to challenge its accuracy if need be; and

10. **Provide Recourse**: organizations are to inform clients and employees of how to bring a request for access, or complaint, to the Chief Privacy Officer, and respond promptly to a request or complaint by the individual.

2.3 The Privacy Officer and Responsibilities

A Privacy Officer is the first point of contact at Spendsafe when it comes to privacy issues. He or she has the authority to intervene on privacy issues and is responsible for overseeing all activities related to the implementation of, and adherence to, the organization's privacy practices, and to ensure operational procedures follow relevant privacy laws, including PIPEDA.

By law, all organizations must assign at least one person as their Privacy Officer. For Spendsafe, Nicksain Kalaimathian has been appointed Spendsafe's Privacy Officer.

As such, the Privacy Officer must be able to do the following:

- Demonstrate knowledge of the organization's personal information handling policies and procedures;
- Demonstrate knowledge of the organization's responsibilities under PIPEDA;
- Explain the procedures for requesting personal information and filing complaints;
- Have the support of senior management and the ability to intervene on privacy issues; and
- Conduct or supervise complaint investigations.

Other responsibilities of the Privacy Officer include:

- Developing and implementing personal information policies and practices.
- Responding to requests for access to and correction of personal information
- Working with the Information and Privacy Commissioner in the event of an investigation
- Complying with all 10 fair information principles.
- Protecting all personal information held by Spendsafe, including any personal information transferred to a third party for processing.
- Conducting Privacy Audits and Impact Assessments, identifying risks and providing corresponding recommendations.
- Training all front-line and management staff on privacy incidents and reporting.
- Maintaining current knowledge of applicable Canadian privacy laws.
- Responding to inquiries from privacy regulators and other government authorities.

3. Personal Information

3.1 Personal Information we collect

Spendsafe will collect the following type of personal information in order to establish a business relationship, offer our product or communicate with our customers:

Cardholders and Guardians (Customers):

Category of Personal Information	Personal Information we collect
Profile and contact Information	• First and last name • Email • Phone number • Address • Unique identifiers (if any) • Financial information (including banking records)
Biometric information	• Faceprints (and facial mapping and scans of digitized images from Onfido)
Sensory information	• Photos, videos or recordings of you and your environment
Identifiers	• First and last name contained on your identification documents • Full address contained on your identification documents • Personal photograph from your identification documents (if applicable)
Demographic information	• Age / date of birth contained on your identification documents • Nationality indicated on your identification documents • Sex indicated on your identification documents • Expiry date of your identification documents • Place of Issuance of your identification documents

Website Visitors

Category of Personal Information	Personal Information we collect
Device/IP information	• IP address • Device ID • Domain server • Type of device / operating system / browser
Web analytics	• Web page interactions • Referring webpage • Non-identifiable request IDs • Statistics associated with the interaction between device or browser and our website
Geolocation information	• IP-address-based location information • GPS data

3.2 Why we collect Personal Information

Spendsafe is an incorporated business entity providing funding access to children through the use of its Spendsafe Visa Reloadable Prepaid Card; which is solely funded through the parents/legal guardian's respective bank accounts or credit cards.

Spendsafe collects personal information on its customers for the following purposes:

1. To establish a business relationship with the customer;
2. To process their transactions.
3. To verify their identity.
4. To collect payment for their use of the Service.
5. To track, improve and personalize our Services, content and advertising
6. To troubleshoot problems with the Service.
7. To comply with applicable laws and regulations, such as those relating to "know-your customer," terrorist financing, and anti-money laundering requirements (PCMLTFA);
8. To detect and prevent fraud and other illegal uses of the Service.
9. To send marketing notices, service updates, and promotional offers.
10. To collect survey information that will be used to monitor or improve the use of our Service and overall customer satisfaction.
11. To comply with the following regulatory and financial partners requirements:
    a. PIPEDA; and
    b. Service providers (banking partners) requirement.

3.3 How we collect Personal Information

Spendsafe may collect customers' personal information directly, from third parties or automatically when a customer visits our digital platforms. Spendsafe may collect information from the following channels:

1. Directly. Through the following:
    a. Application form;
    b. Spendsafe's website; and
    c. Spendsafe's App
2. Third parties: - We can do this with the customer's express consent or as permitted or required by law. For example, obtain customer's personal information from the following categories of third parties:
    a. Credit bureaus
    b. Government institutions or regulatory authorities
3. Public sources such as telephone directories, newspapers, Internet sites, commercially available marketing lists, or government agencies and registries like land or property registries or driver's license offices, or public records as defined by applicable laws
4. Other financial institutions including fraud management purposes
5. Other organizations through business transactions or strategic partnerships. For example, People's Trust Company
6. Third party identity verification and authentication Service Providers. E.g. Onfido

3.4 How we use and share Personal Information

When customers create an account through our website or use our services, we ask them to provide certain personal information as detailed above. We use this information to create and update their account, verify their identity and send communications about their account or assist when they contact customer support.

Personal information will be disclosed to only Spendsafe's employees, senior management and directors who need to know the information for the purposes set out in this Privacy Policy. Personal information will also be disclosed to Service Providers with the individual's knowledge and consent, which may be implied as per this Privacy Policy.

Specifically, when we make reference to sharing information within Spendsafe, we mean sharing personal information within Spendsafe and its Service Providers. E.g. People's Trust Company and Onfido).

We use and share personal information for the following purposes:

Cardholders and Guardians

1. To provide customers with the requested services;
2. To manage their account with Spendsafe;
3. To respond to questions, comments or concerns regarding Spendsafe;
4. To allow for more meaningful and useful marketing initiatives;
5. Establish and authenticate customers' identity and determine their eligibility to use Spendsafe's products and services;
6. Help to ensure that the products and services offered purchased by customers are appropriate for them;
7. Send communications to by postal mail, email, text message, telephone, an automated dialing-announcing device at the numbers provided to us, fax, other telecommunication channels, social media or other methods;
8. Better manage and improve customers' overall relationship with Spendsafe, including monitoring, reviewing, analyzing or improving client services and business processes to make it easier to do business with Spendsafe;
9. Perform everyday business and operations including recordkeeping or internal reporting;
10. Manage Spendsafe's credit, business and other risks so that Spendsafe operates as an effective, efficient and financially prudent program manager;
11. Meet tax, legal and regulatory obligations;
12. Protect Spendsafe and the customers from error and criminal activity, including the prevention, detection and investigation of fraud, money laundering, cyber threats and other such risks and threats; and
13. Such other uses may be permitted or required by applicable law.

Website Visitors

14. We use persistent cookies to measure site and mobile app usage, including browsing behaviour, to improve functionality, and evaluate the effectiveness of our sites, communications and promotional offers;
15. We use location information derived from your IP address from your browser or mobile device and geolocation information (e.g., GPS location) from your browser or mobile device if you have enabled it to share this data;
16. We may also use location information to personalize your user experience, including through site or mobile app content, marketing, or offers for products and services;
17. Such other uses may be permitted or required by applicable law; and
18. Such purposes for which Spendsafe may obtain consent from time to time.

We share customers' information with our Service Providers to help determine the customers' eligibility for a Spendsafe Visa Reloadable Prepaid Card.

3.5 How we keep Personal Information

Spendsafe protects and respects the confidentiality of all information entrusted to the company, except as permitted or required by law, contract or PIPEDA.

Depending on the nature of the information, the customer's personal information may be stored on Spendsafe's server, in our computer systems or in record storage facilities of Spendsafe or its Service Providers.

Information may also be stored and processed in any country where our Service Providers operate. By using our products or services, customers will consent to the transfer of information to countries outside of Canada, including the United States, which may provide different data protection rules. Spendsafe and our Service Providers may perform activities outside of Canada. As a result, customers' information may be securely used, stored or accessed in other countries and be subject to the laws of those countries.

3.6 How long we keep Personal Information

Personal information will be retained in client files as long as the use for which it was collected is active and for such periods of time as may be prescribed by applicable laws and regulations, resolve disputes, or enforce our agreements. Specifically, where Spendsafe is required to keep records in accordance with the AML/CTF requirements, such records will be retained for a period of at least five years following:

1. the termination of the agreement, in respect of business relationships;

2. the day on which the last business transaction is conducted; and

3. the day on which they were created, in respect of all other records.

Where an application has been initiated but not completed, or where Spendsafe has rejected an application, the file and all personal information contained in the file will be retained for a period of six months (except for fraudulent applications – where the five year rule will apply.

Lastly, all records that are required to be maintained under the PCMLTFA are to be retained in such a way that they can be provided to People's Trust Company within 30 days after a request is made. In addition, records may be kept in either machine readable form, if a paper copy can be readily produced from it or electronic form, if a paper copy can be readily produced from it and an electronic signature of the person who must sign the record is retained.

When the customer's information is no longer required, Spendsafe shall securely destroy or make it anonymous.

3.7 How we secure Personal Information

Spendsafe is committed to securing customers' personal information and has taken precautions to protect such information against unauthorized access, loss, theft of information, disclosure, inappropriate alteration, and misuse. We maintain appropriate physical, technical and administrative safeguards to help protect our customers' personal information.

We update our security technology, standards and processes on an ongoing basis. We regularly test and audit our security measures and assess that they remain effective and appropriate. Our employees who have access to customers' information are aware of the importance of keeping it confidential.

Information may be shared with or accessed by our Service Providers so that they can perform services on our behalf. We are always careful when selecting our Service Providers and require them to have privacy and security standards that meet Spendsafe's requirements. We use contracts and other measures to maintain the security of our customers' information and to prevent it from being used for any other purpose other than that for which it was intended.

These are some of the measures we use to protect our customers' information:

- Client information stored electronically is protected by a password. Access to Spendsafe's electronic database is limited on a need-to-know basis for added security.
- Spendsafe does not keep any hard copy client documents.
- Access to client information will be limited to those who need to know the information for the purposes set out in the client's consent or as otherwise permitted or required by law or contract.
- Spendsafe's personnel will never leave client personal information, in paper or electronic form, unattended or exposed to anyone other than the client.
- Spendsafe will not send confidential personal information to clients by email without the client's prior consent. Personal information sent to clients or about clients will employ password protected documents and/or secure email. If clients state they do not wish to receive emails in a secure method Spendsafe's staff will inform clients that Spendsafe does not accept responsibility for communications sent in a non-secure way. This is documented in the client's file.
- Client information transmitted via email to third parties shall be sent in an encrypted format.
- Web-based counselling will use an encrypted platform to protect client privacy and confidentiality.

3.8 How we update Personal Information

Spendsafe makes every reasonable effort to keep our customers' information as accurate, complete, and up-to-date as possible for the purposes in which it is used. However, Spendsafe heavily relies on the customer to update their personal information as soon as it changes.

Customers can update their information through the online account or by calling our customer care service line. Keeping customers' information accurate and up-to-date allows us to continue to offer high quality services.

4. Accessing Customer's Personal Information

Our customers have the right to access their personal information we hold about them. A customer who wishes to review or verify what personal information is held by Spendsafe, or to whom the information has been disclosed (as permitted by the Act), may make the request for access, in writing, to the Spendsafe 's Privacy Officer.

Specifically, we will require our customers to put their request in writing. We will also need to verify their identity before searching for or providing them with access to their information. We will let them know in advance whether there will be a fee to provide access to their information. We may also ask for additional information to confirm the scope of their request, such as the relevant time period or a specific description of the information they are seeking to access.

Once we receive the written request, verify their identity and understand the scope of their request, we will provide a written response to their access request within 30 days, or the timeframe set by applicable privacy law.

If we have obtained information about them from others, they can ask us for the source of that information. On request and where legally permitted, we will provide them with the types of third parties to whom we have, or may have, given their information. However, this will not include Service Providers we have used to do work for us. It will also not include reports to the Canada Revenue Agency, FINTRAC or information that has been provided for legal and regulatory obligations.

For those with a sensory disability, we will endeavour to provide them with access to their personal information in an alternate format, if so requested.

5. Breach and Incident Management Protocols

A privacy breach is an incident involving the unauthorized collection, use or disclosure of personal information. Unauthorized disclosures of personal information are the most common sources of privacy breaches and can occur when personal information is lost, stolen or inadvertently disclosed through human error.

Circumstances that could lead to a privacy breach include:

- loss or theft of equipment containing personal information (e.g., memory sticks, disks, laptops)
- e-mails sent to a wrong address or person
- incorrect file attached to an e-mail
- disposal of equipment containing personal information without secure destruction
- insufficient controls in place to protect personal information in electronic files
- information faxed to a wrong number
- use of laptops, disks, memory sticks or other equipment to store or transport personal information outside of the office without adequate security measures

Upon discovery of a privacy breach or suspected breach, the following steps may need to be carried out simultaneously and in quick succession:

STEP 1: IMMEDIATELY IMPLEMENT PRIVACY BREACH PROTOCOL

- Notify all relevant staff and senior management of the breach, including the Privacy Officer, and determine who else from within the organization should be involved in addressing the breach.
- Develop and execute a plan designed to contain the breach and notify those affected.

STEP 2: NOTIFY OPC IF REQUIRED

- Determine if we are required to report the breach to the Office of the Privacy Commissioner of Canada (OPC). We are required to report breaches to the OPC under the circumstances set out in the PIPEDA regulation; these circumstances are described in the following section: "What you need to know about mandatory reporting of breaches of security safeguards."
- If we are required to report the breach to the OPC, we do so at the first reasonable opportunity, either online or by mail. (See a copy of the OPC reporting form here).

STEP 3: STOP AND CONTAIN THE BREACH

Identify the scope of the breach and take the necessary steps to contain it, including:

- Retrieve and secure any personal information that has been disclosed.
- Ensure that no copies of the personal information have been made or retained by the

individual who was not authorized to receive the information. Their contact information should be obtained, in the event that follow-up is required.
- Determine whether the privacy breach would allow unauthorized access to any other personal information (e.g. an electronic information system) and take necessary steps, such as changing passwords, identification numbers and/or temporarily shutting the affected system down.

STEP 4: NOTIFY THOSE AFFECTED BY THE BREACH

Spendsafe must take the necessary steps to notify those individuals whose privacy was breached, including:

- Identify all affected individuals and notify them of the breach at the first reasonable opportunity. Notification can be by telephone or in writing or depending on the circumstances. There are numerous factors that may need to be taken into consideration when deciding on the best form of notification, such as the sensitivity of personal information.

- When notifying individuals affected by a breach, we must:
  - Provide details of the breach to affected individuals, including the extent of the breach and what personal information was involved.
  - Advise all affected individuals of the steps that we are taking to address the breach, and that they are entitled to make a complaint to the OPC. If we have reported the breach to the OPC, we must advise them of this fact.
  - Provide contact information for someone within the organization who can provide additional information, assistance, and answer questions. (A FAQ document can be developed to assist with this process).

STEP 5: INVESTIGATION AND REMEDIATION

Spendsafe will be expected to conduct an internal investigation, including:

- Ensuring that the immediate requirements of containment and notification have been met.
- Reviewing the circumstances surrounding the breach.
- Reviewing the adequacy of our existing policies and procedures in protecting customers' information.
- Ensuring all staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of PIPEDA.

6. Reporting Privacy Incidents and Complaints

If a customer has a concern about Spendsafe 's personal information handling practices, a complaint, in writing, may be directed to the Spendsafe 's Privacy Officer below:

Privacy Officer
Spendsafe Inc.
50 Minthorn Blvd
Suite 100
Thornhill
ON L3T 7X8

Or

Email: info@spendsafe.ca

When reaching out, customers are encouraged to include their name and contact information, the nature of their complaint, question or concern, details relevant to the matter and the names of any individuals whom they have already discussed the issue with.

Upon verification of the individual's identity, Spendsafe 's Privacy Officer will act promptly to investigate the complaint and provide a written report of the investigation's findings to the individual.

Where Spendsafe 's Privacy Officer makes a determination that the individual's complaint is well founded, the Privacy Officer will take the necessary steps to correct the offending information handling practice and/or revise Spendsafe 's privacy policies and procedures.

Where Spendsafe 's Privacy Officer determines that the individual's complaint is not well founded, the individual will be notified in writing. If the individual is dissatisfied with the finding and corresponding action taken by Spendsafe 's Privacy Officer or the Privacy Officer is unable to resolve the concern, the individual may bring a complaint to the Office of the Privacy Commissioner of Canada (OPC) at the address below:

Office of the Privacy Commissioner of Canada (OPC)
30 Victoria Street
Gatineau, Quebec
K1A 1H3
Telephone: 1-800-282-1376
Website: priv.gc.ca

Last Updated: August 30, 2022.

The End