Privacy Policy

Effective: November 8, 2026 • **Version:** 2026-11-08 • **Service:** SpendLeak

This document describes the conditions under which SpendLeak is offered and should be read together with the other policies published through the Service. The actual service operator and monitored legal contact are identified on SpendLeak's legal information page.

Contents

1. Scope and accountability
2. Categories of account information
3. Categories of Customer Data
4. Collection sources
5. Purposes for processing
6. Consent and lawful authority
7. Where information is stored
8. AI requests and external models
9. Service providers and disclosures
10. Cross-border processing
11. Cookies, tokens and local storage
12. Legal acceptance and audit evidence
13. Retention principles
14. Access and correction requests
15. Deletion and account closure
16. Information security
17. Security incident handling
18. Minors and organizational accounts
19. Marketing choices and anti-spam law
20. Automated processing and meaningful review
21. Accuracy and correction of business records
22. International and regional rights
23. Data processing for business customers
24. Business transfers and corporate changes
25. Policy updates and notices
26. Questions, complaints and accountability

1. Scope and accountability

This Privacy Policy describes how SpendLeak handles personal information in website visits, account registration, use of financial-review workspaces, requests for assistance and the optional AI assistant. The accountable operator is identified through the Service's configured legal identity and contact information. In business workspaces, a Customer may decide why records are collected and how they may be used, while SpendLeak supplies technical processing. Those roles vary with applicable privacy law and the specific activity.

The operator must designate an accountable privacy contact and apply lawful privacy principles, including purpose limitation, appropriate consent or other lawful authority, safeguards, retention limits and access rights where applicable. The policy is not evidence of a security certification. If the actual operator details, practices or vendor arrangements change materially, this policy should be updated and the changes communicated where required.

2. Categories of account information

When you register with email and password, SpendLeak collects the name and email you supply and stores a password-derived hash rather than the password itself. It also stores a unique account identifier and may record the time of registration, authentication events and legal acceptance version. If you use Google, GitHub or Microsoft sign-in, the provider may share a user identifier, display name, email and profile image according to the scopes and settings you approve.

The platform may process session tokens, IP addresses, request metadata, user-agent information, anti-abuse counters and error reports needed for authentication, diagnostics and protection. Those details can constitute personal information when associated with an identifiable individual. We should limit access to such records to people and providers who need them for legitimate operational purposes.

3. Categories of Customer Data

Customer Data may include supplier and customer company names, invoice numbers, dates, service descriptions, quantities, prices, taxes, payment references, contracts, contract amendments, seat counts, credit memos, user notes and review decisions. These records may incidentally identify employees, contractors, sole proprietors, supplier contacts or other people. The Service should not be used as a general-purpose repository for bank credentials, full payment-card numbers, health records, government identity documents or unrelated sensitive personal records.

The Customer is responsible for deciding which records are suitable to upload and for removing unnecessary personal information. Source files may contain metadata or free-text fields beyond the columns used by the detection engine. A person preparing imports should review them before uploading; automatic validation cannot reliably identify every confidential or sensitive value.

4. Collection sources

Information comes from users who enter records, upload files, register accounts or send messages; identity providers that authenticate users; hosting and infrastructure systems that create operational logs; and service providers that return technical responses, such as an AI model when a user requests assistance. The Service does not presently promise automatic extraction of all external bank or accounting information. References to exporting from QuickBooks, Xero and NetSuite describe user-directed file imports unless a separately authorized connector is actually active.

Business records should not be collected by silently accessing a third-party account. If live integrations are introduced, the interface should explain permissions, data categories, processing frequency and disconnection controls before any user grants access.

5. Purposes for processing

SpendLeak uses information to create accounts, authenticate users, provide saved workspaces, accept imports, run comparison rules, display findings, maintain investigation records, provide user-requested AI assistance, respond to support inquiries, prevent misuse, troubleshoot faults, preserve relevant security evidence and comply with applicable law. The operator should not repurpose sensitive business records for unrelated advertising or sale without a lawful basis, adequate notice and any required consent.

Personal information should be collected and used only to the extent reasonably required for the stated purpose. Operational analytics should be minimized or aggregated when possible. If a new product purpose materially changes how information is handled, the operator should assess lawfulness and communicate the change before proceeding.

6. Consent and lawful authority

Acceptance of the Terms is not blanket consent to every conceivable use of personal information. Privacy practices must rest on appropriate consent or another lawful basis applicable to the data and jurisdiction. Where meaningful consent is required, the operator must explain the information collected, the reason for processing, significant risks and available choices in an understandable form. Non-essential collection should be optional and should not be bundled into account creation.

A Customer must have authority to submit information about employees, suppliers or others. Withdrawal of optional consent may stop the related feature but does not always require deletion of records that must lawfully be retained. Marketing consent, if marketing is ever introduced, must be separate from a mandatory Terms checkbox and comply with applicable anti-spam law.

7. Where information is stored

The application can store signed-in customer workspaces in a managed PostgreSQL database when DATABASE_URL is configured. Website files and server-side processing can operate through a cloud hosting provider. Authentication may involve an external identity provider selected by the user. The user-visible browser may also store session and interface information. Browser-only modes depend on the user's device and do not have the same retention or recovery characteristics as a hosted workspace.

Precise data-centre regions, provider subprocessors and disaster-recovery locations are determined by the operator's actual configuration; they must not be represented as exclusively Canadian unless that has been confirmed. Information may be processed outside the user's province or country, where foreign laws may permit access by public authorities.

8. AI requests and external models

When the optional AI assistant is used, the application can send a selected, question-relevant workspace context and the user's conversation text to a hosted third-party model provider to prepare a response. Information sent may contain business names, contract details, invoice references and personal information embedded in records. The assistant is not necessary for the core deterministic detector and should be treated as an optional processing activity.

The provider's processing, logging, retention and training terms are governed by the provider's current contractual and technical settings. We will not assert that provider input is never retained or trained upon unless that statement is confirmed for the active account and settings. Users should not submit unnecessary personal or highly confidential details to the assistant. Output may be inaccurate and should be checked against source documents.

9. Service providers and disclosures

Service providers may include the hosting platform, PostgreSQL provider, identity providers, AI provider when used and email or monitoring services if later configured. Each provider should receive only information reasonably needed for its function and be governed by appropriate contractual, security and confidentiality protections. The operator remains accountable for relevant privacy obligations when using processors and should maintain an up-to-date subprocessor register.

We may disclose information when required by valid legal process, to defend rights, to investigate fraud or security threats within lawful limits, or with authorization from the Customer or affected individual. An acquisition or restructuring might involve limited transfers subject to confidentiality, legality and notice requirements. We do not represent that financial records are sold to advertisers.

10. Cross-border processing

Hosted databases, identity platforms, logging systems and AI providers may process information in countries other than Canada. Privacy law and government access regimes can differ. Where required, the operator should identify material foreign processing locations, assess transfer risks, use appropriate contractual controls and give meaningful notice. A provider's cloud-region selection is not by itself a guarantee that every support, telemetry, backup or subprocessor activity stays in that region.

Customers with contractual or legal data-residency requirements should not assume the current Service meets those requirements without an explicit written confirmation. A written data-processing agreement may specify restrictions, but a publicly posted unsigned template does not create a separate signed service commitment.

11. Cookies, tokens and local storage

Essential session cookies or analogous browser storage may be used to maintain authentication and protect requests. Local or browser-only workspaces may keep information in the browser under the user's control, where clearing site data can remove records. Interface preferences and security tokens may also be stored. The Cookies and Local Storage Notice provides additional information.

The operator should not add optional behavioural advertising, cross-site profiling or non-essential analytics cookies without updating the disclosure and collecting consent where required. Browser controls can affect service functionality. Clearing cookies may sign you out; clearing local storage may delete records saved only on that device.

12. Legal acceptance and audit evidence

The Service records acceptance of a specified Terms and Privacy version and the time and method of acceptance. These records help determine which agreement a user acknowledged. A legal acceptance log is not a substitute for meaningful consent to optional personal-information processing or marketing. Authentication failures may be tracked in limited form to prevent abuse, and workspace review actions may be recorded to preserve the history of user decisions.

Security and audit records should have appropriately restricted access and defined retention. Customers should not treat user-entered recovery entries as independently verified bank records. The operator must avoid retaining unnecessary login or financial data solely because a log exists.

13. Retention principles

We aim to retain personal information only for as long as reasonably necessary for legitimate service purposes and any legal obligations. Account records, workspace data, backups, incident records,

support correspondence and vendor logs may have different retention periods. Retention practices depend on the database, hosting and providers actually configured. We do not claim that an automated deletion process exists where it has not been deployed.

When a workspace or account is closed, deletion may occur in stages and may be limited by outstanding legal obligations, fraud investigations, valid litigation holds or backup cycles. Personal information no longer needed should be securely disposed of or de-identified. Customers remain responsible for keeping any financial records that tax or corporate law requires them to retain independently of SpendLeak.

14. Access and correction requests

Subject to applicable law and identity verification, people may request access to personal information about them, correction of inaccurate information and information about how it has been used or disclosed. Where SpendLeak acts on behalf of a Customer that controls the records, a request may need to be directed to that Customer, with reasonable technical assistance from SpendLeak. We will not disclose one company's confidential records to someone claiming to represent another company.

Requests should be made through the legal/privacy contact listed in the Service. Explain enough to locate the relevant records, but do not send passwords, sensitive documents or full payment-card details by ordinary email. Any refusal or limitation should have a lawful basis and, where required, an explanation and review route.

15. Deletion and account closure

Users may request account closure or deletion of eligible workspace data through the published contact channel where self-service account deletion is not available. The operator must verify the request, distinguish login credentials from workspace records and consider legal retention requirements. Deleting a saved workspace does not necessarily delete the identity-provider account, an external AI provider's logs or existing backups immediately.

We should confirm a completed deletion request to the extent appropriate and disclose meaningful exceptions when legally required. Users must export necessary documents before deletion. A claim of universal deletion or a one-click deletion feature must not be made unless it is supported end to end in the deployed system.

16. Information security

Safeguards appropriate to the sensitivity of stored information can include access controls, password hashing, transport encryption, least-privilege database credentials, input validation, rate limits, incident-response procedures and provider security features. The specific controls implemented in

code may change and do not establish independently verified certification. Secure operation requires proper cloud configuration, vulnerability management, staff procedures and actual incident testing as well as written policy.

No internet platform can promise immunity from intrusion or error. Users should use unique passwords, maintain secure devices and reduce uploaded personal data. Suspected compromise should be reported promptly through the verified contact details.

17. Security incident handling

The operator should investigate credible security events, limit exposure, preserve relevant evidence, assess impacted records and determine whether notice is required by applicable privacy law. Under PIPEDA, qualifying breaches that create a real risk of significant harm may trigger reporting and individual notification requirements; other provincial or contractual rules can also apply. Records of breaches should be retained as required by law, even when notification is not necessary.

The operator will not promise a universal incident-notice deadline that has not been reviewed against applicable law and actual operations. Where required, affected individuals and customers should receive useful details about the incident, its effects and practical mitigation measures without exposing new security vulnerabilities.

18. Minors and organizational accounts

SpendLeak is designed for authorized business-finance review rather than independent use by children. A person creating an organizational account must have sufficient legal authority and capacity to provide the data and bind the organization. The operator should not solicit personal information from children for this purpose and should evaluate age-related consent obligations if it has reason to believe a younger person is using the Service.

Where the operator discovers information was submitted without required authority or consent, it should assess restriction or deletion subject to law and any legitimate business record-retention obligations. An age statement in this policy does not substitute for any age-assurance or guardian authorization controls that applicable law may require.

19. Marketing choices and anti-spam law

Operational messages about account security, requested support and material service changes may be necessary to operate the Service. Promotional or commercial electronic messages, if introduced, require compliance with applicable anti-spam law, including consent or a lawful exception, sender identification and an effective unsubscribe method. Checking mandatory Terms and Privacy boxes is not a marketing opt-in.

If a marketing preference feature is introduced, consent records and unsubscribe requests should be maintained separately. Users must be able to withdraw marketing consent without losing access to functions that do not depend on marketing. The operator must not assume the mere existence of an account gives unrestricted permission to market to it.

20. Automated processing and meaningful review

SpendLeak can use deterministic rules and statistical indicators to prioritize possible billing issues. Such processing is not a final legal decision, credit score or certified audit. Human review remains necessary, particularly if a result could lead to withholding payments, accusing a supplier or changing a contractual relationship. We should document the limitations and data quality of detection rules when materially relevant.

The optional generative AI assistant may create summaries and drafting suggestions, but those outputs may be mistaken. Customers should maintain meaningful human oversight and not treat AI results as independently verified facts. Individuals affected by a consequential decision may have legal rights that cannot be displaced by an automated workflow.

21. Accuracy and correction of business records

The Customer controls the accuracy, completeness and lawful source of imported records. SpendLeak may transform or normalize data to run checks but does not guarantee that every input has been validated. If incorrect personal information is identified, the appropriate controller should correct it and, where required, update downstream records. A financial discrepancy finding is distinct from an error in the personal information relating to an identifiable person.

The operator should preserve reasonable provenance where feasible and avoid overwriting original evidence without record. Users should review field mappings and verify that currency, tax, supplier and invoice identifiers were interpreted correctly before sharing results externally.

22. International and regional rights

Privacy requirements depend on the persons, organizations and jurisdictions involved. Canadian federal and provincial private-sector privacy laws may apply; additional laws may apply to people outside Canada. This policy does not claim universal GDPR, Quebec Law 25 or any particular foreign-law compliance without a factual assessment. If applicable law grants rights beyond those described here, those rights are not restricted by this policy.

The operator should determine its actual markets and processing locations before expanding internationally, provide jurisdiction-specific notices where required and maintain a means to receive and respond to lawful privacy requests. Customers with special industry obligations should obtain a written assessment before using the Service for regulated records.

23. Data processing for business customers

When acting as a service provider processing Customer Data on the Customer's instructions, SpendLeak should process only within authorized purposes, limit personnel access, use suitable subprocessors, assist with relevant rights requests where legally required, support security incident communications and provide deletion or return options to the extent feasible. Detailed contractual commitments belong in a separately agreed Data Processing Addendum when warranted.

A public draft DPA is not automatically executed, and this Privacy Policy is not an assurance of any unattested technical control. Customer organizations remain accountable for giving required notices to their own employees, vendors and other people whose information appears in uploaded records.

24. Business transfers and corporate changes

If the operation is reorganized, acquired or transferred, personal information may be considered for transfer only to the extent permitted by applicable law and the relevant contractual obligations. Any recipient should be subject to appropriate confidentiality and purpose restrictions. Material changes to processing practices should be communicated where required, and necessary consents or other lawful authority should be obtained before data is used for new purposes.

The operator must not assume that selling the software or its source code automatically authorizes unrestricted sale of customer financial datasets. Privacy, confidentiality and trade-secret duties may continue following a business transfer.

25. Policy updates and notices

The policy's version and effective date appear on the Service. A material change should be explained through reasonable notice, and fresh consent should be obtained where required for a new collection, use or disclosure. Minor editorial changes may be made without an individual notice when no substantive right or practice changes. Historical versions should be archived so that acceptance and disclosure records remain understandable.

Continuing to use an account does not automatically authorize unrelated optional data use. We will not present a new marketing or AI-processing purpose as already approved solely because a user once accepted the Terms of Service.

26. Questions, complaints and accountability

Contact the privacy contact displayed in the Service if you have a question, suspect misuse or want to exercise privacy rights. The operator should respond in a reasonable manner, request only necessary identity verification and keep a record of substantive privacy complaints and resolutions. Where

applicable, users may complain to a competent privacy regulator without forfeiting their legal rights by agreeing to contractual terms.

The operator is responsible for providing an accurate legal identity and a monitored privacy contact and for maintaining these published practices as the service changes.

Contact and version control

This document is issued under SpendLeak policy version 2026-11-08. Questions, complaints and authorized requests should be addressed through the legal or privacy contact shown on the deployed Service. The operator must ensure that its public legal identity and monitored contact details are accurate before public use.