# Off Grid Software Privacy Policy

LAST UPDATED **August 2, 2026** SECTIONS **18**
PUBLISHED AT **cink.in**

This is the complete document. The version published at cink.in is the same text, built from the same source, and is the version in force. Section numbering, headings and wording match the web copy exactly.

## 1. Who We Are

Off Grid Software is operated by Deliri Software Inc., located in Scarborough, Ontario, Canada.

In this Privacy Policy, "Off Grid Software", "we", "us", and "our" mean Deliri Software Inc., operating as Off Grid Software. "You" means a visitor, customer, client, user, administrator, developer, employee, contractor, or other person who uses our websites, marketing sites, landing pages, web application, account dashboard, hosted services, APIs, downloadable binaries, support channels, bug, witness, peachfuzz, products, services, or related tools.

## 2. Scope

This Privacy Policy explains how we collect, use, disclose, retain, and protect personal information when you:

- Visit our websites, marketing sites, landing pages, or public pages.
- Contact us, request support, or communicate with us.
- Buy, subscribe to, download, install, activate, register a device for, or use bug, witness, or peachfuzz.

- Create an account, sign in, or use our web application, account dashboard, hosted services, APIs, license systems, update systems, support systems, billing systems, or product telemetry.
- Hire us for websites, applications, APIs, hosting, email setup, maintenance, support, implementation, testing, compliance evidence, or related services.

This policy is intended for business-to-business use. Our products and services are not intended for personal, family, household, child-directed, or consumer use.

Our websites, products, and services are not directed to children. We do not knowingly collect personal information from anyone under the age of majority. If we learn that we have collected personal information from a child without legally required consent, we will delete it.

## 3. Personal Information We Collect

We may collect the following categories of information, depending on how you use our services:

- Contact and account information: name, business email, phone number, company name, job title, billing contact, technical contact, security contact, and support contact.
- Billing and transaction information: invoices, subscriptions, payment status, payment processor records, tax information, billing address, statement descriptors, chargeback records, dispute records, and collection records.
- Business and project information: requirements, repositories, domains, systems, environments, policies, controls, audit objectives, compliance frameworks, project records, support requests, and client-provided materials.

- Product and license information, in these categories: license and entitlement identity (license key, activation status, Organization License, organization identifier, Product, plan, entitlement, and update requests); device and environment identity (device or environment identifier, device label, operating system, IP address, and user agent); build identity (downloaded binaries, Product version, and build hash); one bounded Usage Window (typed command and work-unit counts, aggregate execution and CPU duration, result-class counts, queue or backlog counts, artifact and receipt counts, freshness instants, exact window boundaries, and watermark, never command arguments or customer-controlled names); control-plane response facts (signed Provider Time, closed Product Status, decision kind, generation, nonce, and accepted watermark); and diagnostic and security signals (typed error or crash classes about our binary, activation events, and abuse-prevention events, never raw captured output). We may add, change, or remove individual fields within these categories as the Products develop. What never leaves your systems through a license check-in is stated below and does not change.
- Custody-control information: upload-session identity, nonce, Product, plan, account and organization identity, Registered Device identity, artifact kind and identity, format revision, declared and observed byte size and digest, upload status, validation status, rejection or conflict reason, storage identity, retention class, receipt generation, acceptance time, upload-authorization verifier and bounds, and signed receipts. We do not keep a reusable plaintext object-storage URL after its bounded transfer purpose ends.
- witness evidence and timestamping information: the source-free witness custody projection described below; opaque run and installation identities; hashes and digests; timestamp requests, responses, and tokens; timestamp-authority provider records; certificate chains; verification status; typed request and response times; account, organization, license, and Registered Device identifiers; IP addresses observed by our service; and typed technical, retry, error, and security events about our Product and service.

- bug workflow information: bug records, issue identifiers and content, proof rows, test results and output, command results and arguments, repository and branch names, paths, remote URLs, module paths, commit messages, source code, diffs, and diagnostic logs stay on your systems and in your repositories. bug's license check-ins never transmit them. Where a bug plan includes custody, we receive only the source-free Custody Artifact described in Section 8.1 of our Terms: random repository and device or key identifiers, operation and closure digests, batch commitments, Product and schema revisions, occurred-at time, signatures, timestamp receipts, and the minimum verification metadata required to validate them.
- witness evidence information: where a witness plan includes custody, we receive a sealed, source-free custody projection produced on your machine. It may include only compiler-defined Product, release, schema, policy, profile, tool, and result enums; opaque run and installation identities; bounded counts and durations; ledger, manifest, artifact and report commitments; hashes; timestamp receipts; run attestations; checksums; signatures; and verifier material. It never includes customer-controlled free text, source code, source-derived file contents, names or paths, raw test or command output, reproduction inputs, corpus or crashing inputs, secrets, credentials, production data, personal information, protected health information, full private datasets, or the local human-readable report itself. witness validates the projection against its closed custody allowlist before submission. You keep the complete local bundle and report. witness Local sends no Custody Artifact.

- peachfuzz search information: your source, repository and branch identity, paths, target names, stack traces, test output, and raw run records stay on the machines you run peachfuzz on, and peachfuzz's license check-ins never transmit any of them. Where a peachfuzz plan includes custody, we receive the versioned, signed effort evidence described in Section 9A of our Terms: opaque or content-addressed identities, counting-window boundaries, bounded effort, invocation, target-coverage, candidate-count, unique-finding-count and outcome-class counters, content digests, signatures, timestamps, and the minimum verification metadata required to validate them. That evidence tells us how many findings peachfuzz retained and their content-addressed identities, and carries nothing from which a defect could be reconstructed.

- peachfuzz Cloud Evidence: this is separate, it is off unless you turn it on, and it is the one place where inputs to your own program reach us. Cloud Evidence is available on peachfuzz Attested and Archive and is enabled explicitly in the daemon's configuration. When it is on, each of your machines uploads coverage-increasing corpus entries and the inputs that produced retained findings into storage private to your tenant, so your other machines can start from what one machine already discovered instead of searching the same ground again. That is the whole reason the feature exists: a fuzzer generates an enormous number of inputs, almost none of them interesting, and a second machine is only worth running if it does not repeat the first machine's work. Those uploads are byte strings, predominantly generated by the fuzzing engine mutating earlier inputs, and they contain no source code, file or repository paths, repository or branch names, module paths, command arguments, credentials, secrets, or raw process output. They are derived from the seed inputs you placed in your own repository, so they can carry fragments of whatever you seeded, and a retained crashing input is by definition the data that caused a failure. We hold the encryption keys, so we are able to read an uploaded object. We do not. Our systems process them automatically to store, deduplicate, distribute to your own machines, retrieve, and export them, and our people open one only if you ask us to during a support request, a court orders it, or the law compels it. Because we are able to read them, valid legal process served on us can reach them, and we would rather say that here than let you discover it. Section 9A.1 of our Terms states the same commitments contractually. If your seed corpora are built from real production data, personal information, or regulated data, weigh that before enabling Cloud Evidence, and see Section 15 of this Policy.
- Account and dashboard information: private account, entitlement, Registered Device, upload, receipt, custody, retention, usage, payment-state, export, and verification records used to operate your account and show your organization its own Product state.
- Website and analytics information: pages viewed, referrer, approximate location derived from IP address, device/browser information, cookies, pixels, analytics events, and security logs.

- Communications and project records: emails, support tickets, chat and messaging-app messages including WhatsApp and SMS, ticket and pull request comments, call notes, meeting notes, and, where we make them, recordings and transcripts of calls and meetings. We tell you at the start of a call or meeting if we are recording it, and you can decline, in which case we keep written notes instead. Also feedback, feature requests, complaints, and dispute records.

Our Products are built so that your work stays on your machines. bug, witness, and peachfuzz never transmit source code to us, and our Product control plane never accepts source code. The same exclusion covers source-derived file contents, paths, repository or branch names or identifiers, remote URLs, module paths, command arguments, issue or ticket titles or content, raw test or command output, corpus entries, generated inputs, crashing or reproduction inputs, stack traces, arbitrary evidence contents, secrets, credentials, personal information, protected health information, and other work product except for the exact source-free Custody Artifact fields our Terms expressly admit, and except for the corpus entries and retained finding inputs that Section 9A.1 of our Terms admits on the separate peachfuzz Cloud Evidence channel, which is off unless you enable it. Those two exceptions are the whole of it, they are named in the Sections above, and a category not named there is excluded. This applies to registration, check-in, usage, diagnostics, timestamping, custody, receipts, release, upgrade, Product support telemetry, every version of every Product, and every automated Product route. We will not add a field, configuration escape hatch, support flag, plan, or Order that carries source code through the Product control plane. Section 7A of our Terms of Service states the same commitment contractually.

Product traffic uses direct versioned structures with named identities, closed enums, bounded numbers and durations, typed times, hashes, signatures, nonces, and watermarks. It does not contain generic metadata maps, arbitrary key-value attributes, untyped extension objects, free-form payload strings, opaque telemetry blobs, or catch-all byte fields. We document the admitted field inventory and purpose so a customer inspecting Product traffic can understand what each field means.

Custody is separate and explicit. A custody-eligible Product may submit only the source-free Custody Artifact its Product-specific terms define, through the upload, validation, and signed-receipt flow in Section 7B of our Terms. Starting a subscription, registering a device, checking a license, or enabling telemetry does not authorize us to collect any other work product. bug custody is intentionally source-free, and so is peachfuzz custody: the peachfuzz Custody Artifact carries counters, digests, signatures, and verification metadata only. peachfuzz Cloud Evidence is a different thing on a different channel, described in Section 3 of this Policy and Section 9A.1 of our Terms. It is the only route by which inputs to your own program reach us, it is available only on the plans whose terms include it, and it stays off until you enable it. witness custody contains only the closed source-free projection listed in this Policy and Section 9.1 of our Terms; the complete local witness bundle and human-readable report remain on your systems.

Separately scoped custom Services may require you to grant us repository access or provide source code under a signed Order. That is not Product telemetry or Product control-plane communication. We do not intentionally require secrets, private keys, credentials, health information, payment card numbers, government identifiers, or other highly sensitive information unless a separate signed Services Order expressly requires it through an approved channel.

## 4. Custody Artifacts, Receipts, and witness Timestamping

For a plan that includes custody, the Product first asks our control plane for a short-lived authorization tied to one declared artifact. The Product then uploads that artifact directly to our designated object storage. We inspect the stored object's identity, size, digest, format revision, signatures, and entitlement before accepting it. We store the accepted artifact in object storage, store its validated private account state in our account database, and return a signed receipt. We do not treat upload completion alone as acceptance.

We use custody-control information and accepted Custody Artifacts to provide retention, retrieval, verification, receipts, exports, account dashboards, billing integrity, security, abuse prevention, support, and legal compliance. Identical retries

converge on the same stored artifact and receipt. A different artifact presented under an existing identity is rejected as a conflict and does not replace the accepted artifact.

Custody Artifacts, their metadata, and account statistics are private to the customer account by default. We may publish aggregated or de-identified statistics that do not identify you or reveal confidential information. We do not publish your identity, project or repository identity, findings, artifact metadata, evidence, or account statistics unless an authorized account administrator explicitly enables the exact public field or publication.

witness is designed to help create and preserve evidence records. To do that, witness may need to call an Off Grid Software server. Our server may then call a third-party timestamp authority, certificate authority, or related trust service provider to obtain a timestamp token or timestamp response.

For witness, we may keep records needed to prove, verify, audit, troubleshoot, bill, secure, or reproduce the timestamping process. These records may include:

- The request time and response time.
- The account, Organization License, organization, Registered Device, and opaque run identity associated with the request.
- The evidence hash, digest, opaque identity, or other compiler-admitted source-free timestamping input.
- The timestamp authority selected or used.
- The timestamp token, response, certificate chain, verification status, and related metadata.
- IP addresses observed by our service and typed Product, retry, error, and security events.

witness sends only the exact source-free structures admitted by Section 9.1 of our Terms. It never sends source code, full source files, full private datasets, customer-controlled evidence contents, Regulated Data, secrets, credentials, personal information, or confidential work product through the Product control plane. No Product configuration, support instruction, plan, or Order can expand that automated Product channel. A separately scoped custom Service may receive Client Materials only through the distinct approved channel and signed Services Order described above.

## 5. Downloadable Binaries, Updates, and Activation

bug, witness, and peachfuzz may be distributed as downloadable binaries, CLIs, agents, daemons, or other executable software. Every machine you run one of them on is registered to your account before it does licensed work, and we issue that machine a signed Product Lease naming it. When you download, install, activate, register a device, update, or use those binaries, we may collect information needed to:

- Provide downloads and updates.
- Verify licenses and entitlements.
- Prevent fraud, abuse, unauthorized sharing, and account compromise.
- Maintain compatibility, reliability, security, and auditability.
- Diagnose crashes, defects, installation problems, and support requests.
- Enforce subscriptions, Organization Licenses, Registered Device rules, quotas, and product terms.

Registration uses the Registration Token you obtain from your authenticated account. The Product generates its device signing key locally and sends us the device public key, never the device private key. After successful registration the Product removes the Registration Token from process memory and does not write it into Product state. Our control plane stores the token's one-way verifier, identity, status, issuance and expiry facts, and use history needed to authenticate and audit registration; it does not store a retrievable plaintext copy of the token.

Some product features may not work without contacting our servers. This can include license activation, subscription verification, update checks, witness timestamping, support diagnostics, and abuse prevention.

## 6. How We Use Information

We use information to:

- Provide, operate, secure, support, bill, and improve our services and products.
- Create and preserve witness timestamping and audit records.

- Deliver downloads, updates, licenses, subscriptions, hosting, email support, maintenance, and professional services.
- Respond to support requests, disputes, complaints, and security incidents.
- Verify identity, authorization, account ownership, and payment status.
- Administer trials, including verifying eligibility for one Initial Trial per eligible Product per customer, confirming a valid payment method and business purpose before a trial begins, converting a trial to a paid subscription, and detecting attempts to obtain another trial for the same Product through another plan, account, entity, email address, domain, payment method, or device.
- Detect, investigate, prevent, and respond to fraud, abuse, security threats, product misuse, unauthorized access, chargebacks, and legal claims.
- Maintain accounting, tax, compliance, legal, operational, and business records.
- Keep a record of each project, so that what was asked for, agreed, approved, refused, and delivered can be established later, including in an invoice dispute, an audit, or a legal proceeding. Section 12A of our Terms of Service describes this record.
- Communicate about service changes, invoices, renewals, product updates, incidents, security notices, and administrative matters.
- Analyze aggregated, de-identified, or statistical usage information.
- Enforce our Terms of Service, orders, invoices, licenses, and agreements.

## 7. How We Share Information

We may share information with:

- Hosting providers, cloud providers, database providers, storage providers, logging providers, security providers, monitoring providers, and backup providers.

- Payment processors, banks, card networks, billing systems, tax providers, accountants, collection providers, and dispute-resolution providers.
- Timestamp authorities, certificate authorities, trust service providers, and verification providers needed for witness timestamping.
- Email, SMS, communications, customer support, CRM, analytics, and product operations providers.
- Contractors, advisors, auditors, lawyers, insurers, and service providers who need access to help us provide, secure, bill, improve, or defend our services.
- Law enforcement, regulators, courts, arbitrators, government authorities, infrastructure providers, or third parties when required or permitted by law, legal process, security investigation, abuse investigation, or rights enforcement.
- A buyer, successor, lender, investor, acquirer, or restructuring party in connection with a financing, merger, acquisition, asset sale, insolvency, reorganization, or similar transaction.

We do not sell personal information, and we do not share personal information for cross-context behavioural advertising, targeted advertising, or audience building. We do not run advertising or retargeting pixels on our websites, we do not export contact or visitor data to advertising platforms or data brokers, and we do not make personal information available to any third party for that third party's own marketing purposes. Sharing with the service providers listed above, so they can perform work for us under contract, is not a sale.

We do not intentionally disclose client confidential information publicly except as authorized, required by law, or needed to provide, secure, enforce, or defend our services.

## 8. Cookies, Analytics, and Similar Technologies

Our websites and services may use cookies, local storage, logs, and similar technologies for security, authentication, preferences, analytics, performance measurement, error reporting, fraud prevention, and product operations. We may use website analytics and may embed support, chat, scheduling, or help tools that set their own cookies or local storage in order to work.

We do not use advertising or retargeting pixels, ad-network conversion tags, or audience-building tags, and we do not use these technologies to build advertising profiles or to track you across other companies' websites. If that ever changes, we will say so in this policy, with the "Last updated" date changed, before the change goes live, and we will provide any consent mechanism the law requires.

You can control cookies through your browser settings, but some features, including sign-in and account security, may not work correctly if cookies or similar technologies are disabled.

## 9. Legal Bases and Consent

We collect, use, and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances, including to provide requested products and services, perform agreements, operate our business, comply with law, protect rights and security, and obtain consent where required.

Some collection, use, or disclosure is necessary to provide the product or service. For example, witness timestamping requires communication with our server and may require communication with a timestamp authority. License activation and subscription verification may require communication with our servers.

Where a use is optional, we will provide available choices where practical.

Subject to legal, regulatory, and contractual restrictions and reasonable notice, you may withdraw consent to our collection, use, or disclosure of your personal information by contacting our Privacy Officer. If you withdraw consent, some products, features, or services may stop working or may no longer be available to you, and we may continue to retain and use information where the law permits or requires it.

## 10. Retention

We retain information for as long as reasonably needed for the purposes described in this policy, including service delivery, support, security, timestamp verification, audit trails, billing, tax, accounting, dispute resolution, legal compliance, backup, and enforcement.

When personal information is no longer reasonably needed for these purposes, we delete, destroy, or anonymize it within a reasonable time, subject to the rest of this section.

witness timestamping records may be retained for longer periods because their purpose is to provide durable evidence, verification, audit history, and proof of timing. If a client needs a specific retention period, deletion schedule, or evidence-retention obligation, it must be stated in a signed order, data processing addendum, or product configuration.

Retained Product data is held under a Retention Lease, not as a permanent vault, and Section 21B of our Terms of Service sets out the whole arrangement. Published custody windows range from one year to ten years: bug Attested and witness Bronze up to one year; witness Silver up to three years; bug Archive and peachfuzz Archive up to five years; witness Gold up to ten years; and peachfuzz Attested up to one year. bug Solo, witness Local, and peachfuzz Local have no custody. The applicable term is the maximum custody period available while the account stays paid and in good standing; it is not a promise to hold data for the full term after payment stops unless a prepaid archive Order expressly says so.

The data is stored so that it cannot be deleted before a set expiry date. We set that date six months ahead when an eligible plan is activated, and each monthly payment moves it one month further out, so a paid account always has roughly six months of undeleteable retention ahead of it. That protects you as much as it protects us: whatever happens to the account, including a dispute, your data physically cannot be deleted before that date.

If a payment fails, we email you the same day and our payment processor retries. A missed payment means an invoice still unpaid after those retries, not one retry attempt. After the retries finish, and no earlier than about seven days after the first failure, the Products stop doing new work and keep doing read-only work: witness still verifies evidence already held, bug still opens and audits records already created, and peachfuzz stops, because it is a continuous service with nothing to read back. After about thirty days we email again to say any Custody Artifacts we hold are scheduled for deletion in about sixty days and that you should export them. On the third missed invoice we email to say the account is closed and permanent deletion will follow after the

storage expiry. Paying the overdue amount at any point before deletion restores entitlement and custody automatically; deleted artifacts cannot be restored.

Exporting is your responsibility and you have that whole period to do it. After deletion, data is removed from active systems, indexes, backups, and storage on our ordinary cycles, unless a paid-up archive, legal hold, court order, law, an unexpired storage expiry date, or a signed order requires us to keep it.

We may retain backup, archival, legal, fraud-prevention, chargeback, accounting, and security records even after an account is closed where reasonably necessary or legally permitted.

Some records must be kept for long minimum periods, and we keep them for those periods whether or not you ask us to delete them. These include records we are required to retain by tax, corporate, accounting, anti-fraud, anti-money-laundering, electronic-message, export-control, employment, or other law; records we must keep to establish, exercise, or defend legal claims within the applicable limitation periods; records subject to a legal hold, court order, regulatory demand, subpoena, law-enforcement request, or ongoing investigation, audit, or dispute; records under a technical retention lock that has not expired; and evidence and timestamp records whose whole purpose is durable proof of what existed at a point in time. As examples, transaction, invoice, and tax records are generally kept for at least six years after the end of the relevant tax year, and breach-of-safeguards records are kept for as long as PIPEDA requires.

Where information is subject to one of these mandatory or protective retention periods, we may refuse or defer a deletion request for that information, keep it in restricted or archived form until the period ends, and continue to use it only for the limited purpose that requires its retention. We will tell you when we rely on this section to refuse or defer a deletion request, unless the law or an ongoing investigation prevents us from doing so.

Deleting information from active systems does not immediately delete it from backups, disaster-recovery copies, or immutable archives. Those copies are overwritten or expire on our ordinary backup and retention cycles, and remain protected by this policy until they do.

## 11. Security and Breach Notification

We use reasonable administrative, technical, and physical safeguards appropriate to the nature of the information and the size and scope of our business. Safeguards may include access controls, least-privilege access, encryption, logging, monitoring, backups, vendor controls, secure development practices, and incident response procedures.

No system is perfectly secure. You are responsible for securing your own systems, accounts, credentials, repositories, devices, networks, environments, identity providers, backups, and product configurations.

If a breach of security safeguards involving personal information under our control creates a real risk of significant harm to an individual, we will report the breach to the Office of the Privacy Commissioner of Canada, notify affected individuals as soon as feasible, and notify any other organization or government institution that may be able to reduce or mitigate the harm, as required by PIPEDA. If a provincial or other applicable privacy law also requires breach reporting or notice, we will comply with that law as well.

We keep a record of every breach of security safeguards involving personal information under our control, whether or not it creates a real risk of significant harm, and retain those records for as long as required by law.

If we confirm a security incident that has resulted in unauthorized access to, unauthorized disclosure of, or loss of a business customer's materials or personal information under our control, we will notify that customer without undue delay and in any event within seventy-two hours after confirming the incident, at the security or notice contact on file. The notice will say what we know at the time, including what happened, what categories of information were involved, which systems or products were affected, what we have done, and what the customer may need to do, and we will update it as the investigation develops. Section 25B of our Terms of Service sets out the same commitment contractually. We give that notice so our customers can act quickly; it is not an admission of fault or liability.

If you are a business customer, you remain responsible for assessing and reporting incidents affecting information you control, and for notifying your own users, employees, customers, and regulators as your own obligations require.

## 12. Cross-Border Processing

We operate from Scarborough, Ontario, Canada. Our service providers, infrastructure, timestamp authorities, payment processors, support providers, and other vendors may process or store information in Canada, the United States, or other countries where they or their subprocessors operate.

Information processed outside your jurisdiction may be subject to the laws, lawful access rules, courts, regulators, or government authorities of that jurisdiction.

## 12A. Territorial Scope

We are a Canadian company operating from Ontario. Our products and services are offered to businesses in Canada and the United States. We do not offer, market, target, advertise, solicit, price, localize, or make our products and services available to individuals or organizations in the European Economic Area, the United Kingdom, or Switzerland, and we do not monitor the behaviour of individuals located in those territories. A public web page being reachable from those territories is not an offering to them.

We serve business clients across Canada, including Quebec. Where we handle personal information about individuals in Quebec, Quebec's privacy legislation applies to that information in addition to PIPEDA, and this policy applies to it in full. Section 2B of our Terms of Service states the Ontario governing law, forum, and language terms that a business client established in Quebec agrees to.

Our privacy obligations are those set out in this policy and in applicable Canadian law, including PIPEDA and applicable provincial privacy legislation. We do not act as a controller, processor, or representative under the General Data Protection Regulation, the UK GDPR, or the Swiss Federal Act on Data Protection, and we make no representation that our products and services satisfy those laws.

Business customers must not submit, upload, route, or store personal data of individuals located in the European Economic Area, the United Kingdom, or Switzerland through our products and services, and must not use them to monitor the behaviour of such individuals, unless we have agreed to that use in a signed order and a signed data processing addendum. We offer no such addendum by default and may decline to enter into one. Section 26A of our Terms of Service sets out the corresponding contractual terms.

## 13. Access, Correction, and Requests

You may request access to or correction of your personal information by contacting us. We may need to verify your identity and authority before responding.

We may refuse, limit, or delay a request where permitted by law, including where the request would disclose another person's information, reveal confidential or security-sensitive information, interfere with legal rights, compromise an investigation, or impose disproportionate effort.

If you have a question, concern, or complaint about how we handle personal information, contact our Privacy Officer using the contact information in Section 17. If we do not resolve your concern to your satisfaction, you may complain to the Office of the Privacy Commissioner of Canada or to the privacy regulator responsible for your jurisdiction.

## 14. Client-Controlled Data

For professional services and business customer accounts, the client may control information about its users, employees, contractors, customers, systems, repositories, evidence, logs, and environments. If your information was provided to us by one of our clients, we may direct you to that client for access, correction, deletion, or consent requests.

## 15. Regulated and Sensitive Data

Do not provide health information, payment card data, government identifiers, children's information, highly sensitive personal information, export-controlled data, production secrets, private

keys, passwords, or credentials unless a signed agreement expressly permits it and the required safeguards, addenda, or channels are in place.

## 16. Changes to This Policy

We may update this Privacy Policy from time to time. The "Last updated" date will show when the policy was last changed. If changes are material, we will provide notice through reasonable means, such as our website, account portal, email, or product notice.

## 17. Contact

We have designated a Privacy Officer who is accountable for our compliance with this policy and applicable privacy law.

Privacy contact:

Privacy Officer: Ase Deliri Deliri Software Inc., operating as Off Grid Software 40 Frank Faubert Drive Scarborough, Ontario M1C 5H7, Canada Email: ase.deliri@offgridsoftware.ca

---

**Blink Kernel**
Toronto, Ontario, M1C 5H7, Canada
ase.deliri@offgridsoftware.ca