

Data Processing Agreement

v1.5.0

Last updated: 2026-10-29 Effective date: 2026-10-29

This Data Processing Agreement (DPA) governs Toevan's processing of personal data on behalf of a customer in the course of providing the service. It is incorporated by reference into the Terms of Service and applies whenever Toevan processes personal data as a processor.

This DPA sets out the terms that Article 28(3) of the General Data Protection Regulation (GDPR) requires. Where it conflicts with the Terms of Service on the processing of personal data, this DPA prevails. The factual annexes below (roles, data categories, the data-flow schedule, security measures, retention, and the breach window) state Toevan's actual practice.

Parties and roles

For personal data processed through the product, the customer is the controller and Toevan OÜ is the processor. The customer determines the purposes and means; Toevan processes only on the customer's documented instructions, of which this DPA and the Terms of Service are the initial set.

Customer-directed integrations are not sub-processing. Where the customer connects a third party of their own choosing (GitHub as the source of record, and Slack, Jira, Linear, or Kosli), Toevan sends data to that destination on the customer's instruction. Those providers are the customer's own processors under the customer's own agreements, not Toevan sub-processors. The same applies to the public Sigstore Rekor log, which the customer may opt into and which receives hash-only entries. This distinction is set out further on the [Sub-processors page](#).

Subject matter and duration

The subject matter is the processing necessary to provide the service: connecting to the customer's repository, indexing and analysing source code, gating pull requests, and generating evidence. Processing continues for the duration of the subscription and ends on termination, subject to the deletion and return terms below.

Nature and purpose of processing

Toevan processes the customer's data to: index source code; construct the dependency graph; evaluate deterministic blueprints and constraints; gate pull requests; generate, sign, and store evidence and attestations; and, at the customer's option, run the optional AI features described in the data-flow schedule (suggested AI fixes, AI agents that read the customer's code for a task the customer enables, such as AI code review, the architecture assistant and chat, and code embeddings). Processing is limited to what these purposes require.

Categories of personal data and data subjects

The service processes source code and its contents, which can contain personal data, and account data for the customer's users.

- **Data subjects:** the customer's engineers and other users who hold accounts, and any individuals whose personal data appears in the customer's source code, commit history, or test fixtures.
- **Categories:** commit author names and email addresses; any credentials, secrets, or tokens present in code; any personal data, including special-category data and PII, PHI, or PAN, that the customer's code or fixtures contain; and account identifiers (name, work email, authentication identifiers).
- **Evidence contains personal data.** Because evidence records capture what was analysed, they can include commit author identities and references to the personal data found in code. Toevan processes this only to provide the service and on the customer's instructions; the customer, as controller, holds the lawful basis for the underlying data.

Data-flow schedule (code egress)

This schedule is the authoritative statement of how the customer's source code moves through the service, and is identical in substance to the code-egress statement on the Security page.

Here is exactly how your source code moves through Toevan, and where it does not. The four paths below are the whole picture.

1. Deterministic analysis stays in your boundary

The core of the product is deterministic. Indexing, dependency-graph construction, blueprint evaluation, PR gating, and evidence signing all run on Toevan's own EU infrastructure (Hetzner, Helsinki). No third-party AI is involved in any of it. Your source code is processed transiently to produce the analysis and is not sent outside the Toevan boundary. This path does make outbound dependency lookups, described in path 2. They carry package names and versions, never source code.

2. Dependency checks send package names and versions to public services

To check your dependencies for known vulnerabilities and license terms, and to regenerate lock files for fixes you request, Toevan sends the names and versions of the dependencies it reads from your manifests and lock files, except those it identifies as private (see below), to public services in the United States: the OSV.dev vulnerability database, and the public registries and indexes of the ecosystems involved (the npm registry, pub.dev, and, for Go, the module proxy, the checksum database and the pkg.go.dev license listing, and the Python Package Index when Toevan validates the build of a Python project). Each request carries a package name and a version. It does not carry your source code or the contents of your files.

Toevan filters the private names it can identify: before a lookup is made, a dependency is treated as private, and its name is not sent to OSV.dev, the npm registry, pub.dev, the Python Package Index, the Go module proxy, the checksum database or pkg.go.dev, when any of these holds: its Go module path or npm scope belongs to the same GitHub owner as the repository (github.com/owner/... or @owner); it matches a private pattern configured for the platform (the Go GOPRIVATE, GONOPROXY and GONOSUMDB settings and a dedicated pattern list); it resolves from a private registry named in the repository's .npmrc, .yarnrc or .yarnrc.yml, or in a Dart pubspec_overrides.yaml; it is a git, path or local dependency; or it is a Go module path with no domain. When the default npm registry in the repository's configuration is a corporate proxy, no npm names are sent at all. When a package-manager configuration file (such as .npmrc, .yarnrc.yml or pub-

spec_overrides.yaml) or a go.mod cannot be read, Toevan treats the names of that ecosystem as private rather than guess.

The same filter covers the tools Toevan runs for fixes you request. The Go toolchain is told to treat these names as private, so it does not ask the Go module proxy or the checksum database for them. Lock-file regeneration and build validation for npm, Dart and Python projects are not run when they would name a private dependency to a public registry.

Not checked, and never reported as clear: a dependency that Toevan treats as private is not checked against public advisories, and its license is not looked up in a public registry. The scan says how many were skipped, for example "3 private dependencies not checked against public advisories", and does not show their names. A finding that is already open on such a dependency stays open; it is never marked resolved because the dependency was not checked. Licenses of public dependencies are still looked up in the public registries.

What can still go out: Toevan can only filter what it can identify as private. A private package that none of the rules above recognises, for example a private package under another owner's namespace, with no configured pattern and no private registry in the repository's configuration, looks like a public one, and its name and version are looked up like any other. Source code is never sent. If you need to keep a particular set of names out of these lookups, contact security@toevan.com.

3. Optional AI features can send code-derived context to an EU AI provider

Several optional AI features can send code-derived context to a large language model: AI fix generation, which sends the code context for one specific violation, including when Toevan suggests or opens a fix on a pull request; the AI agents that read your code, such as AI code review, which send the files they read for that task; the architecture assistant and chat, which retrieve and send symbol identifiers (names, kinds, signatures, and paths) for the code your question touches; and, depending on configuration, code embeddings during indexing, which turn symbol text (names, kinds, paths, signatures) into vectors. None of them sends a copy of your whole repository.

Where it goes: these code-carrying calls go to Mistral AI through its EU regional endpoint, under a zero-data-retention agreement, or to your own provider if you configured a key (below). This EU routing is enforced by default at the transport boundary that every Toevan platform AI call passes through: a call that cannot reach the EU route fails closed rather than falling back to a provider outside the EU. Code embeddings run on an in-boundary EU model; under the same enforcement, the fallback that would send embed-

ded symbol text to a provider outside the EU is refused. Mistral may serve a third-party open-weight model on the same EU infrastructure; that model's author receives no data from Toevan and is not a sub-processor.

The US route is on standby: OpenRouter, which routes to Anthropic Claude models in the United States, remains contracted but receives no customer code or code-derived context while EU routing is enforced, which is the production default. It would carry code-derived context again only if that enforcement were switched off.

Bring your own key (Team and above): you may configure your own LLM provider key, in which case these code-carrying calls use your own provider relationship, no code-derived context passes through Toevan's routing at all, and each routing decision is recorded per call, with its route, region and retention status.

4. Evidence and attestations are yours, and verifiable offline

Evidence records and attestations are SHA-pinned and stored append-only in Toevan's EU store, and the same records are written to a toevan/evidence branch in your own repository, so a copy of the proof always lives where you control it.

Attestations are DSSE-signed with ECDSA P-256 (cosign-compatible) and can be verified offline with `toevan audit verify` and `cosign verify-blob-attestation`, with no call back to Toevan. They can optionally be anchored to Sigstore Rekord as hash-only entries: the existence of an attestation becomes publicly checkable, but your code and its content never do. Rekord anchoring is built in and opt-in per organisation; only record hashes are published.

Sub-processors

Toevan engages the sub-processors listed on the [Sub-processors page](#), which states each one's purpose, data categories, location, and status. The customer authorises these sub-processors by entering into this DPA.

Before adding or replacing a sub-processor, Toevan gives at least 30 days' advance notice by email, during which the customer may object on reasonable data-protection grounds. Email is the notice channel; subscribing to changes is described on the Sub-processors page.

The customer objects in writing within the notice period. Toevan and the customer then discuss the objection in good faith, and Toevan may offer a reasonable alternative, such

as not using the sub-processor for the customer's data or a change of configuration. If no resolution is reached within 30 days of the objection, the customer may terminate the affected part of the service by written notice, and Toevan refunds the fees paid for the period after termination.

Where a sub-processor must be replaced urgently to protect the security of the service or of the customer's data, Toevan may do so with shorter notice, given as soon as possible, and the customer's right to object runs from that notice.

Toevan imposes on each sub-processor, by contract, data-protection obligations that offer at least the same level of protection as this DPA, and remains fully liable to the customer for each sub-processor's performance of them.

International transfers

The customer's data is hosted in the European Union. On the deterministic analysis path, source code and personal data do not leave the EU. That path has one outbound flow, the dependency check described in the data-flow schedule: package names and versions are sent to public vulnerability and package services in the United States, after Toevan has filtered out the private names it can identify. A private package that Toevan cannot identify is still looked up by name and version.

Code-derived context from the optional AI features (fix generation, the AI agents that read your code, the architecture assistant and chat, and, depending on configuration, code embeddings during indexing) stays in the EU by default. EU routing is enforced at the transport boundary that Toevan's own platform AI calls pass through: a code-carrying call resolves to Mistral AI through its EU regional endpoint, under a zero-data-retention agreement, or, where the customer has configured one, to the customer's own provider key, and fails closed rather than falling back to a provider outside the EU. Code embeddings run on an in-boundary EU model, and their fallback to a provider outside the EU is refused under the same enforcement. While this enforcement is on, which is the production default, the code-carrying calls that Toevan routes transfer no code-derived context outside the EU.

The US route on standby. OpenRouter, which routes to Anthropic Claude models in the United States, remains a contracted sub-processor but receives no code-derived context while EU routing is enforced. If enforcement were ever switched off, code-carrying calls would route to it again; the transfer safeguard for that path is the provider's data processing agreement, which incorporates the European Commission's Standard

Contractual Clauses. Where the customer uses their own LLM key, no code-derived context passes through Toevan's routing and any transfer is governed by the customer's own provider relationship.

Technical and organisational measures

Toevan maintains the technical and organisational measures described on the [Security page](#), which forms the TOMs annex to this DPA. In summary:

- **Encryption.** TLS at the public edge; column-level AES-256-GCM for sensitive credentials; envelope encryption with a wrapped key-encryption key for bring-your-own-key material; AES-256-GCM for OAuth tokens. Datastore-volume, backup, and integration-secret encryption are being hardened.
- **Tenant isolation and access control.** Shared Postgres schema with row-level organisation scoping enforced on every query; request-boundary authorization from organisation membership and audited support grants; fail-closed; a viewer read-only floor; per-organisation erasure.
- **Credential handling.** Customer credentials are validated live against the provider before storage and never returned to the client (only a masked last four characters are shown).
- **Monitoring.** There is no external error-tracking sub-processor. A self-hosted collector on Toevan's EU infrastructure, with SDK-level scrubbing of source, personal data, and secrets, is being implemented.

Retention of processed data

Toevan retains processed data only as long as needed to provide the service, on the following defaults. These are being made configurable knobs, and automated enforcement (auto-purge at the configured horizon) is being implemented; today evidence is immutable and is not yet deleted automatically at the end of its retention period.

- **Product and customer evidence:** three years by default. This is a floor, not a ceiling: on Enterprise it is configurable per customer and framework, and DORA-adjacent buyers who need five years or more can set that.
- **Operational logs:** 90 days.
- **Security and audit logs:** one year.

- **Error-monitoring events:** 30 to 90 days.
- **Backups:** rolling 30 days.

Account and website (controller) data retention, and the statutory retention of billing records, are covered by the Privacy Policy.

Personal-data breach notification

Toevan notifies the customer of a personal-data breach affecting the customer's data without undue delay, and in any event within 48 hours of becoming aware of it, and provides the information the customer reasonably needs to meet its own notification obligations. The notice goes by email to the customer's administrators and includes, as far as then known:

1. the nature of the breach, including the categories and approximate number of data subjects and of personal-data records concerned;
2. the name and contact details of Toevan's contact point for the breach;
3. the likely consequences of the breach;
4. the measures Toevan has taken or proposes to take to address the breach and to mitigate its possible adverse effects.

Where not all of this information is available at once, Toevan provides it in phases without undue further delay. Toevan does not notify a supervisory authority or data subjects on the customer's behalf unless the customer instructs it to. A notice from Toevan is not an acknowledgement of fault or liability.

Audit rights

Toevan makes available to the customer the information necessary to demonstrate compliance with Article 28 of the GDPR and this DPA, including written answers to reasonable security questionnaires and, where Toevan holds them, third-party audit reports or certifications. The customer relies on this information first.

Where that information is not sufficient, or where a supervisory authority requires it or a personal-data breach has occurred, the customer has the right to audit Toevan's compliance with this DPA, itself or through an independent auditor who is bound by confidentiality and is not a competitor of Toevan. An audit takes place at most once in any twelve

months, except when a supervisory authority requires it or following a personal-data breach, on at least 30 days' written notice, during business hours, within a scope agreed in advance, and without access to other customers' data.

The customer bears its own costs of an audit, and reimburses Toevan's reasonable costs of supporting audits beyond two working days in any twelve months, at rates agreed in advance. If an audit shows that Toevan materially failed to comply with this DPA, Toevan bears its own costs and the customer's reasonable costs of that audit, and remedies the failure without undue delay.

As a supporting control, and not a replacement for these audit rights, the product's own evidence is offline-verifiable: the customer can independently verify signed evidence and attestations at any time using `toevan audit verify` and `cosign verify-blob-attestation`, without relying on Toevan.

Deletion and return of data

Ending a paid subscription does not delete the customer's data: the organisation continues on the free plan. The customer can export its evidence records at any time, in a commonly used, machine-readable format, and may request the return of its data.

The customer's data is deleted when an administrator deletes the organisation in the product, or at the customer's written request. On deletion, Toevan immediately deletes the data derived from the customer's source code: repository clones, caches, and code embeddings. A 30-day recovery period follows, during which an administrator can restore the organisation, for example to export its data. When it ends, Toevan deletes the remaining operational data, including the code graph, findings, settings, integrations, and API keys, with erasure enforced per organisation.

Compliance records are not deleted with the operational data. Evidence records and their attestations, audit logs, and invoices are kept with their personal identifiers removed (the commit author of each evidence record, and the email address, IP address, and browser of each audit-log entry), for the retention periods above and the periods the law requires, such as the accounting records the Estonian Accounting Act requires. The record of the customer's acceptance of these terms is kept as it was made, as proof of the agreement.

Copies in backups are deleted as the rolling 30-day backup schedule above ages them out, and are not restored in the meantime except to recover the service.

On the customer's request, Toevan confirms the deletion in writing, signed by an authorised representative of Toevan OÜ, within 10 business days of completing it.

Evidence written to the toevan/evidence branch in the customer's own repository stays under the customer's control and is unaffected by deletion on Toevan's side, so the customer retains its proof after the relationship ends.

Processor obligations and confidentiality

Toevan, as processor:

1. processes the personal data only on the customer's documented instructions, including with regard to transfers to a third country, unless Union or Member State law requires otherwise, in which case Toevan informs the customer of that legal requirement before processing, unless the law prohibits it;
2. ensures that the persons authorised to process the personal data are bound by confidentiality, by contract or by statute;
3. takes the security measures required by Article 32 of the GDPR, as described in the technical and organisational measures above;
4. engages sub-processors only as set out in the Sub-processors section;
5. assists the customer, through appropriate technical and organisational measures and as far as possible, in responding to requests from data subjects exercising their rights, and forwards to the customer without undue delay any such request it receives;
6. assists the customer in meeting its obligations under Articles 32 to 36 of the GDPR (security, breach notification, data-protection impact assessments, and prior consultation), taking into account the nature of the processing and the information available to Toevan;
7. deletes or returns the personal data at the end of the service as set out under Deletion and return of data;
8. makes available the information and allows the audits set out under Audit rights;
9. informs the customer without undue delay if, in its opinion, an instruction infringes the GDPR or other Union or Member State data-protection law;
10. keeps a record of its processing activities on behalf of the customer as Article 30(2) of the GDPR requires, and cooperates with the supervisory authority on request.

Liability and indemnities

Each party's liability arising out of or in connection with this DPA is subject to the limitation of liability in the Terms of Service, and the limit there applies to this DPA and the Terms together, not to each separately.

Nothing in this DPA limits either party's liability to data subjects under Article 82 of the GDPR, or liability that cannot be limited under applicable law. Where both parties are liable to a data subject for the same damage, each bears the part of the compensation that corresponds to its share of responsibility for the damage, as Article 82(5) of the GDPR provides. This DPA creates no indemnities beyond those in the Terms of Service.

Governing law

This DPA is governed by the laws of Estonia, and disputes are subject to the venue stated in the Terms of Service. The lead supervisory authority is the Andmekaitse Inspektsioon (the Estonian Data Protection Inspectorate).

How this DPA is provided

This DPA is published as a public, standard, signable document incorporated by reference into the Terms of Service, so a customer can review it during procurement without a request.

A signable PDF is available by printing this page to PDF: the print stylesheet renders a clean, chrome-free document suitable for signature. A hosted copy at a stable URL is also available at [toevan-dpa-v1.5.0.pdf](#).

Changelog

v1.0.0 2026-08-25

Initial draft: controller and processor roles with the customer-directed-integrations carve-out, subject-matter and purpose, data categories and subjects, the data-flow schedule (shared verbatim with the Security page), sub-processors with 30-day notice and a right to object, international transfers, the technical and organisational measures annex, retention defaults, a 48-hour breach-notice window, audit rights with offline veri-

fication as a supporting control, deletion and return, and Estonian governing law. Enforceable clause wording was left to counsel.

v1.1.0 2026-09-30

International transfers and the shared data-flow schedule now state that the EU route for code-carrying AI calls is live and enforced by default: such calls go to Mistral AI through its EU regional endpoint under a zero-data-retention agreement, or to the customer's own provider key, and fail closed rather than leaving the EU. OpenRouter (Anthropic Claude models, United States) is on standby and receives no code-derived context while enforcement is on; the Standard Contractual Clauses safeguard applies only if enforcement were switched off. The AI agents that read your code are now listed among the code-carrying features. The hosted PDF moves to v1.1.0; v1.0.0 stays available for any copy signed against it. The purposes of processing now name every optional AI feature, not only suggested AI fixes.

v1.2.0 2026-10-23

The shared data-flow schedule is corrected: deterministic analysis no longer states, without qualification, that nothing leaves the Toevan boundary. It now describes the dependency checks that send package names and versions (including, until private-name filtering ships, the names of private dependencies, and never source code) to OSV.dev and the public package registries, including the Python Package Index during build validation of Python projects. International transfers is corrected to match. The hosted PDF moves to v1.2.0; v1.1.0 stays available for any copy signed against it. Counsel review required before this DPA version is published as binding (international transfers wording).

v1.3.0 2026-10-24

The shared data-flow schedule and international transfers now reflect private-name filtering: Toevan filters the private names it can identify before dependency lookups and reports skipped dependencies as not checked against public advisories, while a private package it cannot identify is still looked up as a package name and version. Source code is still never sent. The hosted PDF moves to v1.3.0; v1.2.0 and v1.1.0 stay available for any copy signed against them. Counsel review required before this DPA version is published as binding (international transfers wording).

v1.4.0 2026-10-26

The data-flow schedule, which embeds the Security page's code-egress statement verbatim, describes Sigstore Rekor anchoring as built in and opt-in per organisation, with

only record hashes published; the earlier wording about its default state is removed. The hosted PDF is regenerated as toevan-dpa-v1.4.0.pdf. Nothing else changes. Counsel review required before this version is published as binding.

v1.5.0

2026-10-29

The enforceable clauses are drafted: the DPA states that it sets out the Article 28(3) GDPR terms and prevails over the Terms on personal data; the sub-processor objection process (written objection, good-faith resolution, termination with a refund of the fees for the period after it), urgent replacement, and flow-down with Toevan fully liable; the breach notice contents of Article 33(3), given in phases where needed; audit (information first, then an audit at most once in twelve months on 30 days' notice; the customer bears its own costs and reimburses Toevan's support beyond two working days a year, unless a material failure is found); deletion as the product performs it (ending a subscription keeps the data; deleting the organisation removes source-derived data at once and the remaining operational data after a 30-day recovery period, while compliance records are kept with personal identifiers removed), backups aged out on the rolling 30-day schedule, and a signed deletion confirmation within 10 business days on request; the processor obligations of Article 28(3)(a) to (h); and liability under the Terms' single limit, with Article 82 GDPR unaffected. The hosted PDF is regenerated as toevan-dpa-v1.5.0.pdf; earlier versions stay available for any copy signed against them.