

Draft: under legal review, not yet in force. This document is published for review. Its terms are not in force and are not offered until the review is complete and the draft marker is removed.

Data processing agreement

Last updated: October 19, 2026

This data processing agreement ("DPA") is part of the agreement between Reverixt Inc., a Delaware corporation ("Reverixt", "we"), which provides Vulkro, and the customer that holds a Vulkro Cloud workspace or publishes to an organisation dashboard ("you"). It applies whenever Reverixt processes personal data on your behalf. Where it differs from the [terms of service](#) on the processing of personal data, this DPA takes precedence.

Sign this copy and send it to contact@vulkro.com; we return it countersigned. The current version is published at vulkro.com/legal/dpa.

1. Roles

You are the **controller** of the personal data processed for you, and Reverixt is your **processor**. Where you are yourself a processor for your own customer, Reverixt is your sub-processor, and this DPA applies in the same way.

The command line tools, the local console and the VS Code extension run on your own machines and do not send your code or findings to us. The account, licence and billing data of the people who sign in to the customer portal is processed by Reverixt as a controller, as the [privacy policy](#) describes; this DPA does not cover it.

2. What is processed

The details of the processing are in Annex 1. In short, Reverixt processes:

- the data Vulkro Cloud reads from the Salesforce orgs and code repositories you connect, as listed on [Vulkro Cloud data processing](#);
- the issues, decisions, comments and activity your team records;
- the names and email addresses of the people you add to a workspace;
- the snapshots you publish with vulkro publish, as listed on [Organisation dashboard data processing](#).

3. Your instructions

We process personal data only to provide Vulkro to you, on your documented instructions. Your instructions are this DPA, the terms, and how you configure your workspace: the orgs and repositories you connect, what you turn on, how long results are kept, and what you export or delete. If we believe an instruction breaks the law, we tell you. If the law requires us to process data in another way, we tell you first, unless the law forbids it.

You are responsible for having a lawful basis to let Vulkro read your orgs and repositories, including the data they hold about your own users and developers, and for telling those people where your

own rules require it.

4. Confidentiality

Everyone at Reverixt who can access your personal data is bound by a duty of confidentiality. Our support team can enter a workspace only while one of your members has granted support access, for a period you choose between one hour and seven days, and every visit is recorded in your activity log.

5. Security

We maintain the technical and organisational measures in Annex 2. We may improve them over time, and we will not reduce the overall level of protection they give.

6. Sub-processors

You authorise Reverixt to use the sub-processors listed on [Sub-processors](#). We impose on each of them data protection obligations that protect your data at least as well as this DPA, and we remain responsible to you for their work.

Before we add or replace a sub-processor that handles your workspace data, we update that page and tell the owners of affected workspaces by email at least 30 days in advance. If you object on reasonable data protection grounds, tell us within that period. We will work with you to resolve the objection; if we cannot, you may end the affected service.

Services you choose to connect (Salesforce, your git host, your notification tools, your AI assistant) are your own tools, under their own terms, and are not our sub-processors.

7. Helping you

Taking into account what we process and the information available to us, we help you:

- **answer requests from individuals.** Most can be met in the product: an admin can export or delete an org, a repository or the whole workspace. If a request reaches us directly, we pass it to you and do not answer it ourselves, unless you ask us to;
- **with data protection impact assessments and consultations** with a supervisory authority, where the law requires them, with the information on our data processing pages and in this DPA;
- **with your security reviews**, by answering reasonable security questionnaires.

8. Personal data breaches

If we become aware of a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to your personal data, we tell you without undue delay. We tell you what we know, what we are doing about it, and who you can talk to, and we keep you updated as we learn more. Telling you is not an admission of fault.

9. Where data is processed

Vulkro Cloud runs on Cloudflare. A workspace's database and stored results are placed by Cloudflare when the workspace is created and are not pinned to a jurisdiction; sign-in data is held by Clerk in the United States. Reverixt and its sub-processors operate in the United States and other countries, so your personal data can be processed outside the country you are in.

Where the law requires a transfer mechanism for personal data leaving the European Economic Area, the United Kingdom or Switzerland, the parties rely on the standard contractual clauses approved for that purpose (for transfers from you to us, the controller to processor module), which are incorporated into this DPA by reference, with Annex 1 and Annex 2 as their appendices. If you need data kept in a particular jurisdiction, tell us before you connect an org or a repository.

10. Audits

We make available the information needed to show that we meet this DPA: this page, our [security overview](#), the data processing pages and our answers to your security questionnaires. If that is not enough, or a supervisory authority requires it, you may audit our compliance once a year, on at least 30 days' written notice, during business hours, at your own cost, by a qualified auditor bound by confidentiality, in a way that does not disrupt the service or expose other customers' data.

11. Return and deletion

You can export your workspace data at any time, including while the workspace is read-only. When you delete a workspace, there is a 14-day grace period, during which any owner can cancel. After it we delete the workspace's application, scan environment, database, results storage, encryption key and sign-in organisation. The final copy we take before deletion is deleted 30 days after it is taken, and because the encryption key is destroyed, the encrypted secrets in it can no longer be read. We keep a minimal record that the workspace existed (the company name and the admin contact).

12. Term and liability

This DPA lasts as long as we process personal data for you. Each party's liability under it is subject to the limits in the terms, unless the law does not allow those limits.

13. Contact

Questions about this DPA, and signed copies: contact@vulkro.com. Data in a workspace you already have: support@vulkro.com. Security incidents and vulnerabilities: security@vulkro.com.

Annex 1. Details of the processing

Item	Detail
Controller	The customer named in the signature block, or the organisation that holds the workspace
Processor	Reverixt Inc., Delaware, USA
Subject matter	Providing Vulkro Cloud and the organisation dashboard

Item	Detail
Duration	For as long as the workspace or the dashboard exists, then until deletion as in section 11
Nature and purpose	Reading the orgs and repositories you connect, scanning them, storing and showing the results to your team, sending the notifications you configure
Data subjects	Your workspace members; the users of your Salesforce orgs; the people who commit to your connected repositories; anyone named in the issues, comments and decisions your team records
Categories of personal data	Names, usernames and email addresses; Salesforce profiles and roles; Salesforce login history, including IP address and country; Setup Audit Trail entries and, where you have them, Event Monitoring logs; commit authors; anything your team writes in issues and comments
Special categories	None intended. Vulkro Cloud does not read your Salesforce business records
Retention	As you configure it in the workspace, within your plan; see Vulkro Cloud data processing , section 12
Sub-processors	As listed on Sub-processors

Annex 2. Technical and organisational measures

- **An isolated tenant per customer:** its own database, results storage, application, scan environment and encryption key.
- **One container per scan,** destroyed when the scan ends. A cloned repository exists only inside that container, for the life of the scan.
- **Strict scan egress:** a scan container can reach only the hosts its job needs.
- **Read-only Salesforce access:** no code path creates, changes, deletes or deploys anything in your org, and no business records are queried.
- **Encryption:** Salesforce tokens, git tokens, webhook secrets and notification secrets are encrypted with AES-256-GCM under the workspace's own key. Stored databases and files are encrypted at rest by the hosting platform, and connections use TLS.
- **Personal data masked by default** in results, reports, exports and the API, for email addresses, usernames, phone numbers and IP addresses.
- **Access control:** built-in and custom roles, members limited to particular orgs and repositories, second-person approval for false positives and accepted risks, optional MFA requirement, email-domain limits, IP allowlist and session timeouts.
- **Workspace API tokens** are shown once, stored only as a hash, scoped, never administrative, and can expire or be revoked.

- **Support access only when a member grants it**, for a limited time, with every visit recorded.
- **An activity log** of connections, scans, exports, member and role changes, triage decisions, rule changes, data settings and support access.
- **Signed, rate-limited webhooks**, checked against each repository's own webhook secret.
- **No AI model** receives your workspace data.

Signatures

Party	Customer	Reverixt Inc.
Company		Reverixt Inc.
Name		
Title		
Date		
Signature		

Vulkro is a product of Reverixt. Reverixt Inc., 8 The Green, STE R, Dover, DE 19901, USA.