disqnect

Security and Data Processing Overview

Disqnect Platform | Service information

DQ-ARCH-EN-001 | Version 1.3 | 25 September 2026

Customer information

This overview explains the service, data flows and current safeguards. Contractual obligations are governed by the agreed DPA and customer service agreement.

Service and responsibility

Disqnect AS, organisation number 936 620 744, is a Norwegian provider of authorised security assessments. Its registered address is Olaf Helsets vei 5, 0694 Oslo, Norway.

Customers define the authorised assessment scope during onboarding. Disqnect Intelligence is authorised to run the agreed tests autonomously. Routine authorised actions do not necessarily require individual human approval. The engagement authorisation establishes permitted systems, test classes, exclusions and stop arrangements; the DPA governs personal-data processing and is not itself permission to test third-party systems.

The standard service handles security-testing data, including observations, findings, conversations, command outputs and evidence needed to review and reproduce findings. Patient records, deliberate health-data processing and classified information are outside the standard scope and require an appropriate separate arrangement. A healthcare customer does not automatically change that scope.

How Disqnect Intelligence operates

1. The platform associates a task with an authorised engagement and its available tools.
2. It selects relevant assessment context for the inference service.
3. The inference service returns analysis or proposed tool calls.
4. Application logic mediates supported actions through permissions and engagement/device controls.
5. Results and evidence are recorded for review, reporting and remediation verification.

A model response or content encountered during testing does not change what the customer has authorised. Scope controls vary by tool: connections are tied to the client environment, but general-purpose commands are not automatically restricted to the agreed target list.

The assessment device operates in the customer environment. A shared device may serve different clients, making engagement-specific routing and scope restrictions important. Assessment history and evidence are stored in the platform database. The device provides the connection to the authorised environment.

Clients can request a stop in the application or contact Disqnect. A stop takes effect after the current tool finishes; it does not forcibly terminate that tool. Configured runtime limits are five minutes for most tools and up to 60 minutes for scans. The engagement must account for this behaviour when choosing permitted tests and operating windows.

Data flow and locations

Flow	Processing
Browser and frontend	Exoscale hosts the application interface and frontend server-side functions in Frankfurt, Germany. Requests include technical metadata; authentication-link URLs can contain tokens.
Device and backend	Com4 provides private cellular/VPN connectivity. Backend application execution is in Frankfurt, Germany, on Exoscale. Provider telemetry and administrative/support access are separate processing paths.
Assessment records	Neon PostgreSQL in Frankfurt, Germany, stores application and assessment history.
Inference	TensorX processes assessment prompts and responses in Dublin, Ireland, and Helsinki, Finland. Inference content is processed transiently, without retention or use for model training.
Authentication email	Resend sends verification/reset links and access codes through Ireland; its terms include US processing/storage.
Support and incidents	Proton Mail handles routine correspondence. Assessment evidence is accessed through the platform. Proton Drive provides restricted incident-document storage. Published Mail/Drive storage locations are Switzerland, Germany and Norway.
External lookups	Standard Shodan API lookups submit target IPs when needed within the authorised assessment scope. Reports and conversations are not submitted in this flow.
Software updates	Cloudflare R2 distributes signed software artifacts. Assessment evidence is stored in Neon.

EU application and database hosting do not mean every processing activity is EU-only. The Supplier and Processing Schedule identifies these boundaries. A stricter regional configuration can be assessed and separately agreed; it is not represented as already available.

Current security measures

Database network access is restricted by an IP allowlist. The application uses a dedicated database account with restricted permissions and no database-administration privileges.

Administrative MFA is enabled for Exoscale, Proton, GitHub, Neon, Netlify, Resend, PRO ISP and Cloudflare. This coverage statement is limited to those services.

Authentication-email tracking is disabled, TLS is enforced, and the sending credential is restricted to its sending purpose and domain.

Release checksums are cryptographically signed. Device hardware includes a TPM; hardware presence alone does not establish active TPM-backed protection.

Recovery and incident handling

The production database has seven-day recovery history and daily snapshots expiring after 14 days. A database restoration test was completed on 20 September 2026, including checks of selected records and relationships. This tested database recovery; full-service disaster recovery was outside its scope.

Disqnect has a documented incident-response procedure and has completed a guided tabletop exercise. Security enquiries reach the person responsible for incident response. Customer notifications and updates are governed by the incident provisions of the signed DPA.

Retention and permitted use

Assessment history supports review, reproduction of findings and remediation. The DPA defines retention, return and deletion obligations for the engagement, including treatment of backup copies. Archiving an assessment is not deletion.

The support-retention procedure specifies deletion of sensitive attachments no later than 30 days after case closure and routine correspondence within 90 days, subject to earlier applicable obligations.

Optional reuse of identifiable or confidential customer assessment content for development or evaluation requires a separate agreement covering purpose, authority, recipients and retention. A provider's no-training setting does not itself authorise Disqnect to reuse customer content.

Assurance and contacts

Security enquiries and requests for supporting evidence can be handled under appropriate confidentiality arrangements. Audit cooperation is governed by the DPA.

Privacy: privacy@disqnect.com. Security: security@disqnect.com.