Data Processing Agreement

Disqnect Platform | Enterprise customer agreement

DQ-DPA-EN-001 | Version 1.4 | 25 September 2026

Standard agreement template

Standard agreement template. This DPA sets out the contractual terms for processing customer personal data. It takes effect when the parties agree this version and the completed customer particulars and annexes in writing. Viewing or downloading it does not create an agreement.

Agreement particulars

Particular	Details
Customer / Controller	**[legal name, registration number and registered address]**
Disqnect / Processor	**Disqnect AS**, organisation number **936 620 744**, Olaf Helsets vei 5, 0694 Oslo, Norway
Main Agreement	**[agreement / order reference and date]**
Effective date	**[To be completed for the engagement]**
Customer privacy contact	**[name or function, email]**
Customer incident contact	Customer-designated point of contact and email recorded during onboarding, as subsequently updated by the Customer. Reference: **[onboarding / order record]**. Additional escalation contact or telephone, if agreed: **[Contact or not applicable]**
Disqnect privacy contact	privacy@disqnect.com
Disqnect security contact	security@disqnect.com; any additional agreed escalation channel is recorded in the Main Agreement
Engagement(s) covered	**[customer environment / order references]**

1. Purpose, roles and precedence

1.1 This Data Processing Agreement, including Annexes A-D (the **DPA**), governs Disqnect's processing of Customer Personal Data when providing the Disqnect platform and the security assessment services specified in the Main Agreement (**Services**).

1.2 **Customer Personal Data** means personal data processed by Disqnect on the Customer's behalf through the Services, including personal data within observations, findings, evidence, communications, prompts, model outputs and operational records. The terms *personal data*, *processing*, *controller*, *processor*, *personal data breach* and *supervisory authority* have the meanings given in the GDPR. **Applicable Data Protection Law** means the GDPR as applicable in the EEA, including its implementation through Norwegian law, and other binding data protection law applicable to this processing.

1.3 The Customer is the controller and Disqnect the processor. If the Customer instead acts as a processor for another controller, Annex A must identify that arrangement and the relevant instructions; Disqnect acts as a subprocessor for that processing and the Customer warrants that it is authorised to appoint Disqnect. The obligations in this DPA apply correspondingly.

1.4 The Customer determines the purposes and essential means of processing, the lawful basis, the permitted assessment scope and the authorised recipients. Disqnect determines technical implementation within those instructions and remains responsible for its obligations as processor.

1.5 Disqnect's processing of its own business contact, invoicing and statutory accounting information for independently determined purposes falls outside this DPA and must be described in its applicable privacy notice. Customer assessment data does not become Disqnect's independent-controller data merely because it appears in a support ticket, security log or model request.

1.6 This DPA prevails over the Main Agreement on personal data processing. Mandatory law and any applicable, duly completed international transfer standard contractual clauses prevail over conflicting terms. Annexes form part of this DPA. The Security and Data Processing Overview is explanatory and does not reduce the commitments in this DPA.

Standard service scope: Disqnect processes security-testing data. Patient records and deliberate processing of health data are outside the standard service and require a separate written agreement before processing. Serving a healthcare organisation does not itself extend this scope.

2. Documented instructions and permitted use

2.1 Disqnect shall process Customer Personal Data only on documented instructions from the Customer, as set out in this DPA, the Main Agreement, the agreed engagement authorisation and subsequent instructions from authorised Customer representatives. This includes instructions concerning recipients and international transfers.

2.2 Processing is limited to delivering, securing, supporting and ending the Services for the Customer as described in Annex A. Disqnect shall not sell Customer Personal Data, use it for advertising, combine it across customers for unrelated purposes, or use it to train, fine-tune or improve general-purpose or shared AI models. Disqnect shall impose corresponding purpose restrictions on inference subprocessors. Any separate training service requires a separate, explicit written agreement before data is used.

2.3 Disqnect shall immediately inform the Customer if it considers an instruction to infringe Applicable Data Protection Law and suspend the affected processing pending clarification. If Union or Member State law applicable to Disqnect requires processing outside the Customer's instructions, Disqnect shall inform the Customer of that requirement before processing unless the law prohibits notice on important public-interest grounds.

2.4 Disqnect shall not materially expand the categories of data, purposes, AI recipients, assessment techniques or processing countries beyond the agreed scope without the applicable instruction and change process. A model response, an external webpage or material encountered during an assessment cannot constitute a Customer instruction.

2.5 The Customer shall establish a lawful basis, provide required notices, obtain necessary permissions to assess the systems and communicate relevant restrictions. This DPA does not itself authorise penetration testing, interception, access to third-party systems or testing outside the engagement scope. Those permissions belong in the engagement authorisation / rules of engagement.

2.6 Disqnect may use anonymous, aggregated service-performance statistics to improve its Services only where they do not identify individuals or Customers, permit their identification by means reasonably likely to be used, or disclose confidential assessment content. Processing Customer Personal Data to create those statistics requires documented Customer instructions. Pseudonymised information remains subject to this DPA. Reuse of identifiable or confidential Customer content for Disqnect's own development or evaluation requires a separate written agreement covering purpose, authority, roles, recipients, safeguards, withdrawal and retention before processing begins. This applies even where a provider does not train on submitted data. This DPA grants no independent right to train or fine-tune shared models or retain development working copies. Disqnect may develop and evaluate its Services using synthetic or laboratory data containing no Customer Personal Data or Customer confidential information.

3. Confidentiality and authorised access

3.1 Disqnect shall restrict access to personnel who need it for the agreed Services and who are bound by contractual confidentiality or an appropriate statutory duty. Confidentiality obligations survive termination.

3.2 Disqnect shall provide appropriate privacy and security instruction, maintain access authorisations, review privileged access and revoke access when no longer needed. Customer data shall not be copied to personal accounts, unmanaged devices or unapproved support services.

3.3 Personnel access, including support and remote administration, is subject to the location restrictions in Annex C. Disqnect shall document the purpose and authorisation of privileged access to Customer Personal Data.

4. Security and service resilience

4.1 Disqnect shall implement and maintain appropriate technical and organisational measures under Article 32 GDPR, taking account of the state of the art, implementation costs, processing characteristics and risks to individuals. The agreed minimum measures are in Annex B.

4.2 Measures shall address confidentiality, integrity, availability and resilience; timely restoration after incidents; and regular evaluation of control effectiveness. Disqnect shall document its risk assessments and material remedial actions.

4.3 Disqnect may improve or replace a measure with an equivalent or stronger measure, but shall not materially reduce the agreed protection during the term. A material reduction requires the Customer's prior written agreement and must remain lawful.

4.4 A cloud provider's audit report or certification is evidence about that provider's assessed service and period. It does not constitute certification of Disqnect, the full platform or the Customer's deployment. Provider assurance does not replace Disqnect's own security obligations.

5. Subprocessors

5.1 The Customer grants general written authorisation to engage the subprocessors expressly identified as approved in the completed Annex C. Authorisation is limited to the entities, purposes and processing arrangements agreed in that annex.

5.2 Disqnect shall perform appropriate due diligence and enter into a binding agreement imposing substantively equivalent data protection obligations, including confidentiality, security, assistance, deletion and transfer safeguards. Disqnect remains fully liable to the Customer for each subprocessor's performance of those obligations.

5.3 Disqnect shall give at least **30 calendar days' prior written notice** to the Customer's privacy contact of an intended addition or replacement. Notice shall identify the legal entity, function, data categories, processing and access countries, safeguards and intended start date, with information sufficient for a reasoned objection. Publishing a revised list alone is not notice.

5.4 The Customer may object on reasonable data protection grounds within **15 calendar days** of notice. The parties shall work in good faith to resolve the objection. The proposed subprocessor shall not process the affected Customer Personal Data while the objection remains unresolved. If no suitable alternative can be agreed, the Customer may terminate the affected Services without an early-termination penalty and receive a pro-rata refund of prepaid unused fees for those Services.

5.5 Disqnect shall maintain an accurate list and make relevant subprocessor contractual and assurance information available for verification, subject to proportionate confidentiality protections. For changes initiated by an existing subprocessor to its own downstream suppliers, Disqnect shall notify the Customer without undue delay after receiving notice, provide the available information and identify the intended start date. The upstream notice period may be shorter than 30 days. The Customer retains a reasonable opportunity to object before the affected processing; if the available notice does not permit that opportunity or an objection cannot be resolved, Disqnect shall arrange an alternative or suspend the affected processing. The termination and refund rights in clause 5.4 apply.

6. Processing locations and international transfers

6.1 The approved storage, inference, backup, support, log and communications locations are those expressly recorded in Annex C. There is no blanket permission for worldwide processing. A requirement for strict EU-only processing must be separately recorded and satisfied across the relevant data flows before that profile is offered.

The current deployment hosts application frontend and backend execution on Exoscale in Frankfurt, Germany, and the production database on Neon in Frankfurt, Germany. These EU hosting locations do not describe all supporting processing: email storage, provider telemetry and support access are separately identified in Annex C. Disqnect is a Norwegian service provider.

Customers may request a stricter regional deployment, including EU/EEA restrictions on specified processing and access. Disqnect will assess technical and contractual feasibility and may offer a separately agreed configuration. Any such commitment must identify the covered services, data, locations, permitted exceptions, implementation date and commercial terms in the order and Annex C, and must be verified before the affected processing begins. This is an option for assessment and agreement, not a representation that a fully EU/EEA-only configuration is currently available.

6.2 Norway is in the EEA but outside the EU. References to the EU and the EEA are not interchangeable. The Customer's selected geographical requirement shall be recorded in Annex A and Annex C.

6.3 Disqnect shall not make a transfer of Customer Personal Data outside the EEA unless instructed or authorised by the Customer and compliant with Chapter V GDPR. Where required, safeguards shall include the applicable European Commission transfer standard contractual clauses, a documented transfer assessment and appropriate supplementary measures. An adequacy decision may be relied on only where valid and applicable to the recipient and processing in question.

6.4 If standard contractual clauses are used, Disqnect shall identify and complete the relevant instrument, module, parties and annexes, and make the relevant evidence available to the Customer. For a processor-to-subprocessor transfer this will ordinarily require the processor-to-processor module where applicable. This DPA is not itself an executed international transfer instrument, and the Article 28 controller-processor clauses are not a substitute for one.

6.5 Remote access by a separate recipient in a third country shall be assessed as a possible international transfer. All remote access remains subject to the agreed geographic restrictions whether or not it constitutes a Chapter V transfer. EU storage alone does not establish compliance with an EU-only processing requirement.

6.6 If a safeguard becomes ineffective or Disqnect cannot comply with the agreed location restrictions, it shall inform the Customer without undue delay, suspend the affected transfer and work with the Customer to establish lawful arrangements or return/delete the affected data.

6.7 The parties shall record the Customer-specific processing geography in Annexes A and C before the affected processing begins. The schedule shall distinguish application execution, inference, primary storage, backups, logs, communications and support or administrative access, and identify any expressly authorised exceptions and applicable transfer safeguards. Availability of the Services to other customers in other regions does not authorise processing of this Customer’s Personal Data outside its agreed locations. Changes remain subject to clauses 2, 5 and 6. An agreed regional deployment is a contractual instruction.

6.8 Disqnect shall review legally binding disclosure demands, seek to limit disclosure to what is required, challenge unlawful demands where reasonably available, and notify the Customer unless legally prohibited. It shall document disclosures and applicable restrictions on notice.

7. Assistance to the Customer

7.1 Taking account of the nature of processing, Disqnect shall assist the Customer by appropriate technical and organisational measures with access, rectification, erasure, restriction, portability, objection and other applicable data subject rights.

7.2 Disqnect shall forward a data subject request relating to Customer Personal Data without undue delay and shall not independently respond on the merits unless instructed or legally required. Disqnect shall provide assistance without undue delay, taking account of the applicable statutory deadline and the information reasonably needed from the Customer. Any impediment shall be promptly explained. Additional response targets may be agreed in the Main Agreement.

7.3 Taking account of processing and information available to it, Disqnect shall assist with Articles 32-36 GDPR, including security assessments, breach handling, data protection impact assessments and prior consultation. Assistance shall include relevant data flows, recipients, locations, retention and control evidence.

7.4 Disqnect shall cooperate with competent supervisory authorities as required by law. Any agreed charge for exceptional assistance must be reasonable, disclosed in advance and must not prevent or delay mandatory assistance; no additional charge applies to assistance caused by Disqnect's breach of this DPA.

8. Personal data breaches

8.1 Disqnect shall notify the Customer **without undue delay and in any event within 24 hours after becoming aware of a personal data breach** affecting Customer Personal Data. The 24-hour limit is the contractual maximum and does not replace the requirement to act without undue delay.

For this commitment, awareness is organisational awareness; internal escalation to a particular person does not restart the notification period.

8.2 Initial notice shall go to the Customer-designated point of contact at the email recorded during onboarding, as subsequently updated by the Customer and referenced in the agreement particulars. The Customer shall keep this contact current. Disqnect shall use any additionally agreed escalation channel where needed. Disqnect shall not delay initial notice while completing its investigation. Information may be supplied in phases as it becomes available.

8.3 Notice shall describe, to the extent known: the nature and timing of the breach; affected systems, data categories and approximate numbers of individuals and records; likely consequences; containment and remediation measures; actions requested of the Customer; and a contact for follow-up. Disqnect shall provide material updates without undue delay and a closure report when the investigation is complete.

8.4 Disqnect shall contain and investigate the incident, preserve relevant evidence, mitigate adverse effects and assist the Customer with its notification assessment. The Customer decides notifications to individuals and authorities, except where law directly requires Disqnect to notify. Disqnect shall not make public statements identifying the Customer without consent unless legally required.

8.5 A security weakness discovered within the Customer's authorised assessment is reported through the engagement process. It is not automatically a breach of Disqnect's processing environment. Where facts also indicate a personal data breach, this clause applies.

9. Information, assurance and audit

9.1 Disqnect shall make available all information necessary to demonstrate compliance and allow and contribute to audits, including inspections, by the Customer or its mandated independent auditor.

9.2 The parties may begin with relevant documentation, questionnaires and independent assurance reports. These do not remove the Customer's right to an inspection where necessary to verify compliance. Ordinary audits shall be coordinated on reasonable notice; urgent audits following a material incident, reasonable evidence of non-compliance or a supervisory-authority requirement shall not be delayed by an ordinary notice period or annual frequency limit.

9.3 Audits shall protect other customers' information and use proportionate confidentiality and access arrangements. Disqnect may provide redacted records or controlled review of sensitive technical material where those arrangements still permit effective verification. Protection of intellectual property shall not prevent legally required disclosure or frustrate the Customer's audit rights. Source code, proprietary prompts and testing playbooks are not routine procurement deliverables.

9.4 Disqnect shall address substantiated findings within risk-appropriate agreed periods and provide evidence of remediation. Audit cost allocation, if needed, shall be agreed reasonably and shall not make statutory audit rights ineffective.

10. Retention, return and deletion

10.1 Disqnect shall retain Customer Personal Data only for the purposes and periods in Annex D and documented lawful instructions. Archiving an engagement is not deletion.

10.2 At the end of Services, the Customer may choose return followed by deletion, or deletion without return. Disqnect shall make agreed exports available securely, cease unnecessary processing and delete remaining copies within the deadlines in Annex D, unless applicable Union or Member State law requires storage. Any legally required retention shall be explained, limited to the required data and period, isolated and protected.

10.3 Deletion covers databases, conversation and assessment workflow records, evidence, local device copies, exports, support material, logs where applicable, and subprocessor-held copies. Backup expiry and restoration handling are addressed in Annex D. Disqnect shall ensure that restoring a backup does not reintroduce data that should remain deleted into ordinary processing.

10.4 On request, Disqnect shall confirm completion in writing, identifying any remaining backup or legally retained copies and their final expiry dates. A deletion confirmation shall not claim completion while material copies remain unaccounted for.

11. Term, suspension and termination

11.1 This DPA begins on its effective date and remains in force while Disqnect or its subprocessors process Customer Personal Data. Confidentiality, protection and deletion obligations continue as necessary after the Main Agreement ends.

11.2 Where Disqnect cannot fulfil this DPA, it shall promptly inform the Customer. The Customer may require suspension of affected processing until compliance is restored. If the breach is material and cannot be remedied within a reasonable agreed period, or if continued processing would be unlawful, the Customer may terminate the affected Services. Clauses concerning lawful instructions, urgent suspension and subprocessor objections remain applicable.

11.3 Amendments shall be documented and agreed by authorised representatives, except updates expressly permitted under this DPA. Neither an online policy update nor a unilateral architecture change overrides agreed instructions.

11.4 Governing law, competent courts and contractual liability arrangements follow the Main Agreement to the extent permitted by law. Nothing limits data subjects' statutory rights, supervisory-authority powers, mandatory GDPR liability or rights under applicable transfer clauses.

Annex A - Processing description and instructions

A1. Service and processing

Subject matter: provision of the Disqnect platform, customer-site assessment devices, authorised security validation, evidence management, AI-assisted analysis, customer reporting and associated support.

Purposes: identify and explain security exposures within agreed environments; validate findings and remediation where authorised; maintain an accountable assessment record; enable authorised customer access and communication; and secure, support and conclude the Services.

Nature: collection and recording from authorised systems and devices; transmission; organisation and storage; querying and analysis, including inference; controlled retrieval and display; generation of reports; disclosure to approved recipients; and export, restriction and deletion. Autonomous processing may occur within an authorised engagement. This is not permission for unrestricted testing or general employee surveillance.

Operating model: the Customer sets the assessment scope through application onboarding; the Disqnect Intelligence system is authorised to run the agreed tests autonomously. The Security and Data Processing Overview describes tool-specific scope controls and stop behaviour. Routine in-scope tests do not require separate per-action approval unless agreed for the engagement. The onboarding authorisation and rules of engagement must identify the authorised targets, permitted test classes, exclusions and applicable limits. Scope selection does not itself authorise access to systems the Customer has no right to test. The engagement record shall identify the authorising person, scope/version, acceptance time and subsequent changes. Patient-data handling is excluded from this standard service and requires a separate written agreement. Testing production OT or medical systems requires explicit engagement authorisation and applicable safety arrangements.

Duration and frequency: for the engagement / subscription and agreed wind-down period in Annex D. Processing may be continuous, scheduled, event-triggered or user-initiated according to the agreed engagement settings.

A2. Individuals and information

Category of individuals	Personal data potentially processed
Customer personnel and authorised users	Names, work email addresses, role/access records, authentication and session information, customer messages, instructions and support correspondence
Employees, contractors and other users of assessed systems	Usernames, account identifiers, directory attributes, device and network identifiers, activity timestamps and security-relevant log entries
Customer contacts, suppliers or end users appearing in authorised evidence	Limited content of records, screenshots, files or communications encountered when demonstrating an exposure; only to the extent necessary and authorised
People whose nearby wireless devices are observed, if that assessment is expressly enabled	Wireless identifiers, advertised device attributes and time/location context that may identify or single out a person; exclude or minimise out-of-scope observations

Security findings, IP/MAC addresses, device names and service metadata can be personal data when linked to individuals. Assessment evidence may also contain passwords, tokens, hashes, certificates, configuration details or other highly confidential information. Credentials are sensitive security material even when they do not fall within Article 9 GDPR.

Special categories and criminal-offence data: intentional processing of Article 9 or Article 10 data is excluded unless expressly described and authorised in a supplemental instruction with a lawful basis and additional safeguards. If incidentally encountered, Disqnect shall limit collection, restrict access, avoid unnecessary onward transmission or inference, notify the Customer and obtain instructions for redaction, segregation or deletion. Incidental discovery does not create permission for continued bulk collection.

A3. Engagement-specific authorisation

Complete before processing:

- Systems, network boundaries, locations and authorised device placements: **[Signed rules-of-engagement reference]**.
- Assessment modes, operating windows, excluded assets and prohibited activities: **[To be completed for the engagement]**.
- Authority for active testing, credential use, exploitation, wireless observation and collection of proof: **[To be completed for the engagement]**. Unlisted intrusive activities are not authorised by this DPA.
- Human approvals, pause/stop procedure and emergency contacts: **[To be completed for the engagement]**.
- Approved inference service and permitted input categories: **[To be completed for the engagement]**.
- External intelligence lookups, client-selected connectors and email recipients: **[identify any transfer of domains, IPs, emails or evidence]**.
- Required geography: **[specified EU countries; EU/EEA; or specified locations with authorised transfers]**. Complete a per-service location schedule in Annex C, including failover, backups, logs, email and support access, and any expressly authorised exceptions. Confirm the deployment can meet this instruction before enabling the affected processing.
- Customer role and any upstream controller: **[To be completed for the engagement]**.
- Disclosure/export recipients and designated instruction-givers: **[To be completed for the engagement]**.

Disqnect shall use the least intrusive evidence sufficient for the agreed purpose. Customer credentials and unrelated personal content shall be excluded from AI requests and external lookups unless necessary for an expressly authorised task with appropriate safeguards. Neither automated redaction of all content nor anonymisation of all inference inputs is assumed.

A4. Additional deployment requirements

The standard engagement covers authorised IT security testing. Production operational technology, medical-device testing, deliberate patient-data processing, classified information and deployments requiring security accreditation require a separate written scope and appropriate safeguards before processing. The parties shall identify applicable sector requirements, information classification, geographical restrictions and safety arrangements. Customer sector membership and supplier certifications do not establish acceptance of a deployment.

Annex B - Technical and organisational measures

This annex sets the contractual security requirements for the engagement. The Security and Data Processing Overview describes the current service controls and their scope. Additional deployment-specific measures must be expressly agreed; this annex is not an independent certification.

Control area	Agreed minimum measure
Governance and personnel	Named security and privacy owners; documented procedures; confidentiality duties; appropriate training; recorded access approvals and timely removal of access

Control area	Agreed minimum measure
Identity and access	Unique identities; least privilege; separation of customer viewers, operators and administrators; MFA for privileged access to Exoscale, Proton, GitHub, Neon, Netlify, Resend, PRO ISP and Cloudflare; periodic access review; controlled service credentials. Inference-provider account MFA is not included in this coverage and requires a separately assessed access arrangement
Customer separation	Engagement-bound authorisation of customer access; server-side checks; restrictions on customer-facing assessment tools; testing of cross-customer access boundaries; controlled support access
Transmission	Encrypted application communications over HTTPS/TLS and secure device channels; certificate validation; management connectivity restricted to authorised endpoints; protection of database connections
Storage and secrets	Encryption at rest for customer-data stores and backups; protected encryption keys and application secrets; no secrets embedded in client code; defined rotation/revocation process; specific protection for captured credentials
Device security	Controlled provisioning and restricted administration; authenticated cloud connections; release artifacts with cryptographically signed checksums; controlled recovery and decommissioning. TPM hardware is present. Active TPM-backed protection, secure boot and persistent device-storage protection are not committed by this standard annex
Cellular connectivity	Contracted Com4 private connectivity configured for the deployed devices; customer-specific routing and any geographical requirements recorded for the connectivity service; encrypted application transport across the full device-to-service path
AI processing	Approved inference recipients and regions; purpose and no-training restrictions; task-relevant context selection; control of alternative providers and failover; prompts and outputs treated as customer data; tool access mediated by application permissions
Assessment control	Documented customer authorisation; configured engagement/device scope; restrictions on prohibited activities; recorded approvals where required; documented pause/stop procedures. A stop prevents further tool execution after the current tool finishes; it does not forcibly terminate that tool. Runtime limits are five minutes for most tools and up to 60 minutes for scans
Logging and monitoring	Security-relevant access and activity records; restricted log access; monitoring and incident escalation; avoidance of unnecessary secrets or personal content in logs; defined retention. No immutable-log guarantee is implied
Secure development	Reviewed changes; dependency/vulnerability checks; separated development and production access; risk-prioritised remediation; periodic security testing and recorded outcomes
Recovery	Documented backup scope and retention; protected backups; tested restoration; agreed recovery objectives; prevention of deleted-data reintroduction after restore
Incident handling	Documented response procedure and accountable owner; breach assessment, containment, evidence preservation, notification and review in accordance with clause 8
Disposal	Documented export/deletion workflow across application, device and supplier copies; verification of completion and backup expiry; secure sanitisation before device reassignment
Supplier assurance	Appropriate supplier contracts and risk review; verification of relevant assurance scope, report period and exceptions; maintained supplier/location inventory and transfer safeguards

Configured recovery baseline: seven-day production database recovery history and daily snapshots with 14-day expiry. The completed database restore exercise covered an isolated branch and selected data-integrity checks. No numerical full-service recovery-time or recovery-point SLA is granted by this DPA; any such SLA must be agreed in the Main Agreement.

Additional requirements: the parties may agree stronger access controls, fixed regional processing, independent testing or device protections in a deployment-specific schedule. Such commitments must identify the covered services and be satisfied before the affected processing begins. No amendment may reduce protection below Applicable Data Protection Law.

Annex C - Subprocessors and processing locations

C1. Authorisation

The completed schedule shall identify the approved legal entities, purposes, data categories, processing and access countries, retention and applicable transfer safeguards. Customer authorisation is recorded through agreement to the completed annex; this public template does not itself grant authorisation.

The signed schedule shall distinguish primary storage, backups, logs, support and remote administration. The initial register and subsequent changes are subject to clauses 5 and 6.

C2. Supplier register

Provider / service	Data and purpose	Processing locations and boundaries
Akenes SA (Exoscale), Switzerland - application hosting	Application frontend and server-side functions, assessment API, background processing and application logs	Application frontend and backend: Frankfurt, Germany. Provider administration may involve Switzerland. Provider telemetry and support processing are distinct from application hosting and selected-country data storage.
Neon / Databricks - database (entity as identified in the applicable account agreement)	Application accounts, findings, conversations, evidence and remediation history	Primary production database: Frankfurt, Germany. Configured recovery history: 7 days. Daily snapshots: 14-day expiry. These periods do not describe all provider-level residual copies.
TensorX Ltd., Ireland - AI inference	Assessment prompts and responses, including selected context and evidence	Inference is processed in Dublin, Ireland, and Helsinki, Finland. Inference content is processed transiently, without retention or use for model training.
Plus Five Five, Inc. (Resend) - authentication email	Recipient addresses, verification/reset links and portal access codes	Sending region: Ireland. Provider terms include US processing/storage. Email/log retention on the current plan: 30 days; backup and account-termination periods are separate. Tracking is disabled and TLS is enforced.
Proton AG, Switzerland - support email	Support contacts and correspondence; assessment reports and raw evidence are accessed through the platform	Published Mail storage locations: Switzerland, Germany and Norway; encrypted backups up to 30 days. Ancillary support processing is separate from mailbox storage.

Provider / service	Data and purpose	Processing locations and boundaries
Proton AG, Switzerland - incident records	Restricted incident templates and case-specific records where necessary	Published Drive storage locations: Switzerland, Germany and Norway; encrypted backups up to 30 days. Case-specific access and retention apply to incident evidence.
Com4 AS, Norway - SIM/private VPN	Device/SIM identifiers, connectivity metadata and traffic transport	Private cellular/VPN connectivity. This schedule does not establish fixed countries for network termination, roaming or administrative access; country restrictions require agreement for the connectivity service.
Shodan - standard API lookup	Occasional target-IP queries and associated API-account/request metadata	Target-IP lookups through the standard API. Assessment reports and conversations are not submitted in this flow. Query-associated metadata is logged by the provider. No fixed processing-country or query-retention commitment is established in this schedule. Customer-specific restrictions must be resolved before enabling the lookup for that engagement.

Optional development processing - separate opt-in: use of identifiable or confidential Customer assessment content for Disqnect's own development or evaluation requires separate, recorded Customer authorisation and an agreement under clause 2.6 before processing. It is not included in standard assessment processing. OpenAI Codex Business is the intended development service; Anthropic is not a current provider and any future use requires separate authorisation and provider review. The Supplier and Processing Schedule distinguishes these optional purposes and other infrastructure or website services. Listing a service does not authorise processing.

Hosting locations: application frontend and backend execution and the primary production database are in Frankfurt, Germany. Transactional email is sent through Ireland. Supporting processing includes US email processing/storage and separate provider administration and telemetry. These locations do not constitute an EU-only processing commitment.

C3. Optional services and independent recipients

Domain registration: PRO ISP provides domain registration and renewal; DNS is managed through Netlify. Any expansion to processing Customer Personal Data on the Customer's behalf is subject to the applicable authorisation and supplier requirements.

External intelligence queries can disclose target domains, IP addresses or individual identifiers even when the returned source is public. Their use requires the scope and recipients to be resolved in Annex A. Customer-directed exports and connectors require identified recipients and a clear allocation of responsibility. A Customer choice of a destination does not make Disqnect's own processing exempt from this DPA.

Payment providers may process business billing information as independent controllers or under separate processor arrangements, depending on the actual service. The applicable arrangement shall identify the provider's role and permitted data.

Approved deployment record reference and date: [To be completed for the engagement]. **Customer approval of initial register: [To be completed for the engagement]**.

Annex D - Retention, return and deletion schedule

D1. Retention schedule

The following periods apply when this DPA is agreed. Disqnect remains responsible for meeting them whether a task is performed manually or automatically.

Data class	Retention and deletion rule
Engagement findings, reports and necessary evidence	Retain for testing history for the duration of the Customer agreement, subject to periodic minimisation and earlier lawful deletion instructions. On termination, provide a 30-calendar-day secure export window and complete deletion from active systems within the following 7 calendar days (no later than day 37 after termination), subject to applicable legally required retention.
Assessment workflow records, full testing conversations and raw command outputs forming the evidence trail	Retain the necessary, coherent testing history for review and reproduction of findings for the duration of the Customer agreement, under documented Customer instructions. Apply the same 30-calendar-day termination export window and subsequent 7-calendar-day active-system deletion deadline as reports and evidence, subject to earlier lawful deletion instructions and applicable legally required retention. Credentials and unnecessary sensitive content require separate handling; evidence integrity does not authorise unrestricted retention of such content.
Other raw captures and high-risk proof not required for the retained testing history	Use the smallest sufficient sample. Delete within 30 days of collection unless a documented, time-limited evidence need is agreed.
Credentials, tokens and secrets collected during testing	Where necessary to substantiate and review findings, original credential evidence may form part of the retained testing history under documented Customer instructions and the same export/deletion schedule. Restrict access to Disqnect operators assigned to the relevant Customer and Customer-designated, verified company owners or personnel with an evidence-review or remediation need; use only within the authorised testing scope. Notify the Customer of exposed credentials and recommend prompt rotation or revocation through the remediation workflow. Retention of evidence does not authorise continued use of a credential or require it to remain valid. Remove or redact content when no longer necessary, subject to lawful instructions and applicable retention obligations.
Local device assessment data	The device is not intended as a persistent assessment-evidence store. Any assessment content in temporary files, operational logs, swap or crash dumps remains subject to the applicable minimisation and deletion obligations. Software, configuration and identity material have their own operational purposes
Optional improvement-analysis working copies	Only where separately authorised under the agreed improvement terms. Delete customer-derived working copies, linkable derivatives and associated analysis-session content within 30 calendar days of creation, subject to earlier applicable deletion obligations. Do not reset expiry by copying or reprocessing. Original assessment evidence follows its separate schedule. This row does not itself authorise improvement processing
Operational/security logs	Rolling retention of 90 calendar days for Disqnect-controlled operational/security logs, with payload minimisation. Shorten where justified; document any specific incident evidence retention separately.
Support tickets, diagnostic attachments and routine support correspondence	Delete sensitive diagnostic attachments when no longer needed and no later than 30 calendar days after issue closure. Retain routine support correspondence for up to 90 calendar days after closure where needed. Apply any earlier applicable Customer deletion or termination deadline; document separately any lawful retention exception or incident-evidence need.

Data class	Retention and deletion rule
Inference-service content	No provider retention of prompt/output content after completion and no model training under the agreed inference-service terms. Any exceptions, optional storage and separate metadata retention shall be specified in the completed supplier schedule. Disqnect's own stored context/output remains subject to the rows above
Backups, snapshots and point-in-time recovery history	Following active-system deletion, residual Customer data may remain only until the relevant backup expires under its documented schedule. Current Disqnect-configured Neon history is 7 days and scheduled snapshots expire after 14 days, as confirmed by Disqnect. Restrict residual copies to recovery and reapply deletion instructions before restored data returns to normal service. Do not create retained copies that circumvent expiry.

These limits do not authorise retention of unnecessary data until a deadline. An approved legal hold must identify its legal basis, exact data, access restrictions and end/review date. General service improvement is not a legal hold.

D2. Exit procedure

1. Authenticate the Customer's instruction and agree export scope, format and authorised recipient. Export formats shall include machine-readable structured records and ordinary report/document formats, with a manifest of included and excluded material.
2. Stop scheduled processing, revoke unnecessary access and revoke relevant device/connector credentials at the agreed cut-off.
3. Transfer the export securely, or record the Customer's decision to delete without return. If no instruction is received, provide the agreed export window and delete on the contractual schedule after notice.
4. Delete active data, local device copies and applicable supplier copies; record backup expiry and legal exceptions.
5. Provide written confirmation within five business days after active deletion, stating any copies still awaiting expiry; confirm final completion on request after those copies expire.

Signatures

The parties approve this DPA and its completed Annexes A-D. The agreement particulars, referenced engagement records and any customer-specific schedules form part of the execution version.

For the Customer	For Disqnect
Legal entity: **[To be completed for the engagement]**	Legal entity: Disqnect AS, 936 620 744
Name and title: **[To be completed for the engagement]**	Name and title: **[To be completed for the engagement]**
Signature: _____	Signature: _____

For the Customer	For Disqnect
Date: _____	Date: _____