

Data Processing Agreement

How we protect your information during security testing

Security assessments can expose highly sensitive information: source code, credentials, infrastructure details, personal data and vulnerability evidence. This agreement sets out how Trixent must handle that information, how the Client authorises testing, and what happens when information is exposed, retained, transferred or deleted.

This DPA is designed for incorporation into a signed Services Agreement. It is not effective merely because it has been downloaded or reviewed. The engagement-specific processing details and approved Sub-processor Register must be incorporated before the relevant processing begins.

Version control: v1.8 is a revised working draft. A prior signed version is not amended or replaced unless the parties expressly incorporate this version through their agreed amendment process.

A guide for the Client

This page is a navigation aid. The numbered clauses and incorporated schedules contain the operative terms; this summary does not override them.

Client question	Where the agreement answers it
What Trixent may do	Process Client Personal Data only for the agreed Services, under documented instructions and applicable law.
How information is protected	Apply the agreed controls, including encryption, access restrictions, secure transfer, minimised evidence collection and controlled use of external services.
When you will be notified	Trixent must notify the designated Client incident contact within 24 hours after becoming aware of a qualifying Security Incident.
Who else may process data	Only Sub-processors identified in the approved, dated register incorporated for the engagement.
How long data is kept	Raw artefacts, reports, other confidential material and backups have separate, defined retention periods.
What happens on conflict	The DPA controls personal-data processing; the RoE controls technical scope; required transfer instruments control the transfers they govern.

1. What this agreement covers

1.1 Services covered

This DPA applies when Trixent processes Client Personal Data on the Client’s behalf while providing the services described in the executed Services Agreement and Statement of Work (SOW). The services may

include vulnerability assessment and penetration testing, application and API testing, mobile security testing, internal and external network testing, cloud and infrastructure assessments, source-code reviews, retesting, reporting and other agreed cybersecurity services.

1.2 Client Personal Data

“Client Personal Data” means personal data that Trixent processes on the Client’s behalf in connection with the Services. It may be supplied by the Client or encountered within authorised systems, test accounts, logs, network captures, requests, responses, screenshots, findings and reports. The term has the meaning given by the Applicable Data Protection Law.

1.3 Confidential Engagement Data

“Engagement Data” means information Trixent receives, accesses, generates or produces while delivering the Services. It includes Client Personal Data and other confidential technical or business information, such as source code, network diagrams, infrastructure configurations, credentials, scan outputs, traffic captures, screenshots, logs, vulnerability findings, proof-of-concept material, reports, remediation recommendations and retest results. Engagement Data may be confidential even when it is not personal data.

1.4 Security Incident

“Security Incident” means an actual or reasonably suspected event that compromises the confidentiality, integrity or availability of Client Personal Data or Engagement Data held by or under the control of Trixent or an authorised Sub-processor. It includes unauthorised access, disclosure, loss, alteration, destruction or compromise of credentials. A routine alert or blocked attempt is not automatically a Security Incident if it has not compromised the relevant information, but it must be assessed under the applicable incident procedures.

1.5 Personal Data Breach

“Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, as defined by the applicable data-protection law. A Security Incident may affect confidential Engagement Data without constituting a Personal Data Breach. The contractual notification duties in Section 9 apply as stated there, while statutory notification duties remain governed by applicable law.

1.6 Other terms used

“Services Agreement” means the executed master services agreement or equivalent commercial agreement that incorporates this DPA. “SOW” means the Statement of Work. “Rules of Engagement” or “RoE” means the signed document defining the authorised targets, activities, methods, testing windows and restrictions. “Sub-processor” means a third party engaged by or on behalf of Trixent to process Client Personal Data on the Client’s behalf.

1.7 Applicable Data Protection Law

“Applicable Data Protection Law” means the data-protection and privacy laws that apply to the relevant processing, including the Digital Personal Data Protection Act, 2023 and rules made under it to the extent in force and applicable, the Information Technology Act, 2000 and the SPDI Rules, 2011 where legally applicable, the GDPR or UK GDPR where those laws apply, and any binding cybersecurity, incident-reporting, retention or international-transfer requirements that apply to a party or the relevant systems.

2. Who is responsible for what

2.1 The parties' roles depend on the processing

Where the Client determines the purposes and means of processing and Trixent processes Client Personal Data on the Client's behalf, the Client acts as controller or Data Fiduciary, as applicable, and Trixent acts as processor or Data Processor, as applicable. The parties' actual roles depend on the facts and Applicable Data Protection Law, not merely on the labels used in a contract.

2.2 Trixent's own business records

Trixent acts independently for its own business administration, including its own contact records, quotations, invoices and accounts, where it determines the purposes and means of that processing. Those activities are governed by Trixent's Privacy Policy and applicable law, rather than by the Client's processing instructions under this DPA.

2.3 Engagement-specific processing details

Annex A describes the default subject matter, duration, nature, purpose and categories of processing. The SOW may specify engagement-specific details or changes. Any change to a DPA obligation must identify the exact clause being changed and be expressly agreed in writing by authorised representatives; a general reference to the SOW does not silently amend this DPA.

2.4 Client authority to test

The Client represents that it owns, or is legally authorised to authorise testing of, each asset in scope; that the person approving the engagement has authority to bind the Client; and that all permissions required from third-party owners or providers have been obtained. The Client shall provide reasonable written evidence of that authority when requested. Trixent shall not begin testing an asset until it has verified, to its reasonable satisfaction, that the necessary authority exists.

2.5 Scope, restrictions and readiness

Before testing begins, the Client shall disclose material restrictions or risks that may affect the Services, including sensitive or regulated data, localisation requirements, sector-specific controls, production-critical systems, prohibited techniques, third-party provider terms and recovery limitations. The SOW and RoE shall identify the authorised assets, testing windows, permitted methods, exclusions, source addresses where relevant, report recipients and emergency contacts. For production or higher-risk testing, the parties shall agree proportionate readiness steps; the Client shall maintain appropriate backups and a recovery method and identify an emergency contact reachable during the testing window.

2.6 Scope changes and stop conditions

Changes to targets, testing windows, techniques, report recipients or other security-sensitive instructions require written approval through the agreed change-control process. Trixent may verify a sensitive change by calling back the contact identified in the RoE using previously agreed contact details; an email alone need not be accepted unless it is part of the parties' agreed and verified approval process. Trixent shall not conduct denial-of-service or other disruptive activity without separate prior written approval. If testing reaches an out-of-scope asset, Trixent shall stop the activity that could access or affect it, record only the

minimum information needed to explain the issue and seek written direction before proceeding. Trixent may suspend testing if an unresolved readiness issue creates unreasonable risk.

3. How Trixent may use Client information

3.1 Documented instructions

Trixent shall process Client Personal Data only on the Client's documented instructions in the Services Agreement, SOW, RoE, this DPA or later written instructions issued through the agreed contact process, unless Applicable Data Protection Law requires otherwise. Where the law permits, Trixent shall inform the Client before processing as legally required. If Trixent reasonably believes an instruction infringes Applicable Data Protection Law, it shall inform the Client unless prohibited by law and may suspend the affected processing until the issue is resolved.

3.2 Purpose limitation

Trixent shall use Client Personal Data and confidential Engagement Data only to perform the Services, comply with lawful instructions, meet applicable legal obligations, or establish, exercise or defend legal claims relating to the Services where permitted by law. Trixent shall not sell Client Personal Data, use it for independent marketing, combine it with other clients' engagement data for unrelated purposes, or reuse it in another engagement.

3.3 No training or general improvement from client material

Trixent shall not use Engagement Data, including findings, reports, evidence, credentials or source code, to train, fine-tune or improve an AI model or general-purpose tool. Trixent shall not submit Engagement Data to an external AI service unless the Client has given prior written approval for the engagement and the provider, purpose, data categories, processing location and safeguards have been documented in the approved Sub-processor Register or other incorporated written approval. An approved provider must not train on the Client's material or use it for unrelated purposes.

3.4 Anonymised statistics

Trixent may retain its pre-existing tools, methods and general know-how. It may use engagement-derived statistics for benchmarking or product improvement only with the Client's express written permission and after effective anonymisation such that the Client, its systems and individuals are not identifiable by means reasonably likely to be used. Pseudonymised information remains personal data where it can be linked to an individual.

3.5 Data minimisation

Trixent shall seek to demonstrate findings using the minimum information reasonably necessary, including synthetic indicators, minimal samples or redacted evidence where practicable. Trixent shall not intentionally extract or retain complete production datasets merely to demonstrate a vulnerability.

4. Confidentiality, ownership and disclosure

4.1 Confidential handling

Trixent shall protect Client Personal Data and confidential Engagement Data against unauthorised access, use or disclosure. Personnel who access the information must be bound by appropriate confidentiality obligations and receive relevant security and data-handling instructions. Access shall be limited to those who need it to perform the Services.

4.2 Ownership and licence rights

The Client retains its rights in data, information, source code, systems and materials it supplies or makes available. The rights in client-specific reports, findings and other deliverables created by Trixent are determined by the SOW or Services Agreement. Trixent retains ownership of its pre-existing tools, templates, methods and general know-how, subject to any licence expressly granted in the Services Agreement. Nothing in this clause reduces the confidentiality, security, authorised-use or deletion obligations in this DPA.

4.3 Disclosure required by law

Trixent shall not publish or disclose the Client's identity, reports, findings or other confidential Engagement Data without the Client's written authorisation, except where disclosure is required by law or a binding legal order. Where legally permitted, Trixent shall give the Client notice before disclosure, disclose only what is legally required, and take reasonable steps to protect confidential information.

4.4 Public references and case studies

Trixent shall not identify the Client, publish engagement findings, use client-specific evidence in marketing, or create a case study from an engagement without the Client's prior written consent. Any permitted material must be reviewed and anonymised as agreed before publication.

5. Security measures and encryption

5.1 Required baseline

Trixent shall implement and maintain the technical and organisational measures in Annex C for systems and people used to provide the Services. Measures shall be appropriate to the sensitivity of Engagement Data, the risks of the processing and the scope of the engagement. The controls in Annex C are contractual requirements, not claims of certification.

5.2 Encryption at rest

Trixent shall protect Client Personal Data and confidential Engagement Data stored on systems used to provide the Services, including applicable workstations, storage systems and backups, using AES-256 or equivalent-strength encryption appropriate to the data and risk. Full-disk encryption shall be enabled on devices that store persistent copies of Engagement Data.

5.3 Encryption in transit

Trixent shall protect Client Personal Data and confidential Engagement Data transmitted over public or otherwise untrusted networks using TLS 1.2 or higher with a secure configuration. TLS 1.3 shall be preferred where supported. SSL and TLS 1.0 and 1.1 shall not be used to protect such transfers. Sensitive reports, credentials and evidence shall be sent only through approved encrypted channels with appropriate access controls.

5.4 Key and secrets management

Trixent shall restrict access to encryption keys and secrets to authorised personnel and systems that need them for legitimate operational purposes. Where technically feasible, keys shall be stored separately from the data they protect. Keys must be securely generated, protected and rotated, replaced or revoked when required by the documented procedure, including when compromise is suspected. Trixent shall use an established managed key-management service, secrets manager or equivalent protected mechanism where appropriate to the systems used. Keys and secrets shall not be hard-coded in application source code or committed to version-control repositories.

5.5 Changes to controls

Trixent may update its security measures where the change does not materially reduce the agreed level of protection. A material reduction affecting the engagement requires prior written notice and consultation with the Client. Where a required control is unavailable or a material gap cannot be addressed by an appropriate safeguard, the affected processing shall not begin or shall be suspended until the parties agree a lawful solution in writing.

6. Personnel, access and engagement separation

6.1 Need-to-know access

Trixent shall use individual accounts for personnel who access Engagement Data, apply least-privilege permissions and require multi-factor authentication for accounts that can access Engagement Data. Phishing-resistant MFA shall be used for privileged access where supported and appropriate to the relevant system. Shared accounts shall not be used for routine individual access.

6.2 Access removal

Trixent shall remove or adjust a person's access as soon as reasonably practicable and no later than one business day after the person leaves the engagement, leaves the team or changes role. Access shall be reviewed when personnel join, change roles or leave, and periodically during longer engagements.

6.3 Separate workspaces and devices

Trixent shall keep each engagement in a separate, access-controlled workspace, protected by encryption. Engagement Data shall not be stored on publicly accessible website infrastructure. Devices used to store Engagement Data must use full-disk encryption, screen locking, security updates and endpoint protection appropriate to the system and risk. Shared or public computers must not be used for engagement work.

6.4 Logging and oversight

Trixent shall maintain appropriate records of access to Engagement Data and engagement activity, including testing source addresses and timing where relevant to client correlation. Logs shall be protected against unauthorised access or alteration and retained in accordance with the agreed schedule and applicable law.

7. Sub-processors and subcontracted testing

7.1 Approved Sub-processors

Trixent may use a Sub-processor to process Client Personal Data only if that provider is identified in the approved, dated Sub-processor Register incorporated into this DPA or the applicable SOW. The Register must identify the provider's legal name, role, relevant data categories, processing and storage locations, remote-access locations where relevant, and applicable transfer mechanism or restrictions. A provider is not approved merely because it appears in an internal template or is used elsewhere by Trixent.

7.2 Register availability

Trixent shall provide the applicable Register to the Client before processing begins and maintain its current version. If no Sub-processor is authorised for the engagement, the Register shall state that no Sub-processors are authorised. A missing Register does not authorise a provider to process Client Personal Data.

7.3 Notice of changes

Trixent shall give the Client at least 30 days' prior written notice before adding or replacing a Sub-processor. The notice shall identify the provider, its role, relevant data categories and processing locations. The Client may object during the notice period on reasonable data-protection grounds.

7.4 Objections

The parties shall work in good faith to resolve an objection. Trixent shall not use the proposed provider for the affected processing while a timely objection remains unresolved. If the objection remains unresolved after a further 30 days, the parties shall consider a lawful alternative, suspend the affected processing or terminate the affected part of the Services. Any refund of prepaid fees for Services not provided shall be handled under the Services Agreement. No party is required to continue processing in breach of applicable law.

7.5 Sub-processor obligations

Trixent shall impose written data-protection obligations on each Sub-processor that provide protection materially consistent with this DPA for the processing performed. Trixent remains responsible for selecting and overseeing its Sub-processors and remains liable for their performance to the extent required by applicable law and the Services Agreement. Where GDPR Article 28(4) applies, its requirements apply.

7.6 Subcontracted testing

Trixent shall not engage a third party, including an individual contractor who is not Trixent personnel, to perform testing or access Client Personal Data or confidential Engagement Data without the Client's prior

written consent. This requirement is separate from the approval process for Sub-processors that provide supporting infrastructure or services.

8. Processing locations and international transfers

8.1 Agreed locations

Trixent shall process Client Personal Data only in the countries or regions identified in the approved Sub-processor Register or expressly agreed in the Services Agreement or SOW. Where relevant, the documentation shall identify storage, backup and remote-access locations. Trixent shall not move Client Personal Data to a new country in a way that materially changes the agreed arrangement without the notice and approval required by the Services Agreement or applicable law.

8.2 Client restrictions

The Client shall tell Trixent in writing about localisation, sector-specific or transfer restrictions known to it. Before processing starts, the parties shall assess those restrictions against the proposed arrangement. Trixent shall not proceed with processing it knows would breach a binding legal requirement or an agreed location limit. If a conflict arises during the engagement, the parties shall suspend the affected processing while they determine a compliant arrangement.

8.3 Required transfer instruments

Where an international transfer requires an approved transfer mechanism, the parties shall complete and execute or validly incorporate the applicable instrument before the transfer. Depending on the transfer, this may include the EU Standard Contractual Clauses, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another legally recognised mechanism. A general reference in this DPA does not replace the full and properly completed instrument where one is required.

8.4 Transfer details and safeguards

The parties shall identify the correct transfer instrument and complete the required party details, processing and transfer descriptions, technical and organisational measures, Sub-processor information and assessments. The applicable transfer instrument prevails over conflicting terms for the transfer it governs. Each party remains responsible for the transfer obligations that apply to it.

9. Security Incidents and notification

9.1 Client notification deadline

Trixent shall notify the Client without undue delay and, in any event, no later than 24 hours after becoming aware of a Security Incident affecting or reasonably suspected to affect Client Personal Data or confidential Engagement Data held by or under its control, including through an authorised Sub-processor. The deadline does not depend solely on when a designated contact reads an email. Trixent shall maintain an escalation route capable of receiving and acting on relevant incident reports outside ordinary business hours.

9.2 Initial notice

The initial notice shall include, to the extent known at the time:

- The nature and approximate timing of the incident.
- The affected systems and categories of information.
- The likely consequences.
- Containment measures taken or proposed.
- The contact responsible for incident coordination.

Trixent may provide details in stages as the investigation progresses. It shall not delay the initial notice solely because all facts are not yet known.

9.3 Containment and investigation

Trixent shall take reasonable steps to contain and investigate the incident, preserve relevant evidence, document material findings and cooperate with the Client on mitigation and recovery. Where testing reveals an attacker already present in the Client's environment, Trixent shall stop the affected testing, preserve the minimum evidence reasonably necessary, notify the emergency contact promptly and await instructions before taking remediation actions outside the authorised scope.

9.4 Legal notifications

Each party is independently responsible for notifications and reports that Applicable Data Protection Law or other binding law requires it to make to regulators, authorities or affected individuals. The Client's right to decide its own notifications does not restrict Trixent from meeting its independent legal obligations. Where law permits, Trixent shall notify the Client before making a disclosure that identifies the Client; otherwise, it shall notify the Client as soon as legally permitted.

9.5 Costs and cooperation

Each party shall bear reasonable incident-response costs to the extent caused by its own breach of this DPA, negligence or wilful misconduct, subject to the Services Agreement, the agreed liability limits and applicable law. Where more than one cause contributed, costs shall be allocated according to each party's responsibility. Costs not attributable to a party's breach or fault shall be allocated under the Services Agreement.

10. Privacy requests and compliance assistance

10.1 Forwarding individual requests

If Trixent receives a request from an individual concerning Client Personal Data, it shall forward the request to the Client without undue delay and, where reasonably practicable, within three business days. Trixent shall not respond substantively on the Client's behalf unless instructed or required by law. Nothing in this clause extends a statutory deadline applying to either party.

10.2 Assistance

Taking into account the nature of the processing and the information available to Trixent, Trixent shall provide reasonable assistance to enable the Client to respond to requests for access, correction,

completion, erasure or other rights under Applicable Data Protection Law. Assistance beyond the agreed Services may be charged at the rates stated in the Services Agreement, except where prohibited by law or where the parties agree otherwise.

10.3 Compliance, impact assessments and regulator enquiries

Trixent shall provide information reasonably necessary to demonstrate compliance with this DPA and reasonably assist the Client, where applicable, with security obligations, incident response, data-protection impact assessments, prior consultations and regulator enquiries to the extent they relate to Trixent's processing and the information is available to Trixent.

10.4 Limits of information available

Trixent is not required to identify a person from data it does not hold or reasonably cannot link to an identifiable individual. Where it holds relevant information, it shall provide reasonable assistance, subject to identity verification, security restrictions and lawful retention obligations.

11. Retention, return and deletion

11.1 Credentials and test accounts

At the end of testing, Trixent shall disable or remove credentials and test accounts under its control when no longer needed and confirm completion where specified in the RoE. The Client remains responsible for revoking accounts and credentials under its control.

11.2 Raw testing artefacts

Trixent shall delete raw testing artefacts, including scan outputs, captures and proof-of-concept files, within 30 days after delivery of the final report. Where a retest is agreed and the Client's documented instructions permit retention, Trixent may retain only the raw artefacts reasonably needed for that retest and shall delete them within 30 days after the retest is completed, but no later than 90 days after delivery of the final report unless the Client approves a longer period in writing or applicable law requires retention. If an agreed retest cannot be completed within that 90-day period, the parties must document the necessary extension before the deadline.

11.3 Final reports and limited engagement records

Unless the SOW expressly specifies a different period, Trixent may retain the final report, redacted evidence summary, signed authorisations and relevant engagement activity logs for up to 12 months after delivery of the final report for agreed retests, follow-up questions and disputes. A different period must be stated expressly in the SOW or another written agreement incorporated into the Services Agreement. Retention of a report does not independently authorise processing of personal data contrary to the Client's lawful instructions or applicable law.

11.4 Other client-provided confidential information

Client-provided confidential Engagement Data not covered by Sections 11.2 or 11.3, including source code, architecture material and working files, shall be returned or securely deleted no later than 30 days after delivery of the final report, unless a different period is expressly agreed in the SOW or retention is

required by applicable law. The parties shall not use this clause to extend the permitted retention of raw testing artefacts.

11.5 Return or deletion on request or at the end of Services

At the end of the Services, Trixent shall, at the Client's choice, return or securely delete Client Personal Data processed on its behalf and delete existing copies, unless Applicable Data Protection Law requires storage. Any agreed retention of personal data under Sections 11.2 or 11.3 remains subject to the Client's documented instructions and applicable law; where the Client lawfully instructs earlier return or deletion, Trixent shall follow that instruction. For other Client-provided confidential Engagement Data, Trixent shall follow the periods in Sections 11.2 to 11.4 or any expressly agreed shorter period in the SOW.

For an earlier deletion request, Trixent shall remove the affected information from active systems within 10 business days unless a legal hold, mandatory legal-retention obligation or retention period expressly agreed for a defined purpose in the SOW requires otherwise. Where continued retention is permitted and necessary, Trixent shall identify the material category, reason, access restriction and expected deletion date, unless legally prohibited from doing so.

11.6 Backups and archived copies

Backups and archival copies shall be access-restricted, protected against ordinary use and deleted through a documented lifecycle within 30 days after deletion from active systems. Backup copies shall not be restored or used except for disaster recovery or legal compliance. If a backup is restored, the applicable deletion instructions shall be reapplied. A system that cannot meet the agreed backup-expiry period must not be used for the affected Engagement Data unless the parties agree a written, legally permissible variation before processing begins.

11.7 Legal holds

Where a dispute, claim or legal obligation reasonably requires preservation, Trixent may retain only the information relevant to that purpose, restrict access and use, and inform the Client unless the law prohibits notice. Trixent shall review the hold periodically and delete the retained information when the reason for retention ends.

11.8 Deletion confirmation

On reasonable written request, Trixent shall confirm the deletion actions completed and identify any material category retained and the reason. A deletion confirmation shall accurately describe the actions taken and shall not claim that every backup or provider-held copy has been physically purged while copies remain within the documented backup-expiry period.

12. Audit and assurance

12.1 Information to demonstrate compliance

Trixent shall make available information reasonably necessary to demonstrate compliance with this DPA and shall cooperate with proportionate audit requests relating to the processing covered by it.

12.2 Routine audits

The Client may audit Trixent's compliance on at least 30 days' written notice, normally no more than once in any 12-month period. The audit shall begin with available documentation and remote review where sufficient, and shall be conducted during normal business hours by an independent auditor bound by confidentiality. Its scope must be proportionate and must protect other clients' information and Trixent's security-sensitive systems.

12.3 Additional audit after an incident or concern

An additional audit or shorter notice is permitted where reasonably necessary following a Security Incident, a material documented compliance concern, a binding request from a competent authority or a requirement of Applicable Data Protection Law. Nothing in this clause limits a competent authority's rights under law.

12.4 Costs and assurance materials

Where relevant independent assurance materials reasonably demonstrate compliance, Trixent may provide them in place of duplicative audit work, subject to the Client's legal rights. The parties shall agree reasonable audit logistics and costs in advance. Audit costs shall be allocated under the Services Agreement; where an audit identifies material non-compliance by Trixent, Trixent shall reimburse the Client's reasonable audit costs to the extent agreed or required by applicable law.

13. Liability and responsibility

13.1 Each party's responsibility

Each party remains responsible for its own compliance with Applicable Data Protection Law and for its acts and omissions under this DPA.

13.2 General liability cap

Except as provided in Sections 13.3 and 13.4, each party's aggregate liability under or in connection with this DPA arising from a particular engagement shall not exceed the total fees paid or payable under the SOW giving rise to the claim. Claims arising from the same or related facts shall be aggregated for purposes of this cap. This limit applies only to the extent permitted by applicable law.

13.3 Enhanced cap for confidentiality and data-security failures

The aggregate liability of either party for claims arising from its breach of confidentiality obligations, unauthorised use or disclosure of Client Personal Data or confidential Engagement Data, or a Security Incident caused by that party's breach of this DPA shall not exceed twice the total fees paid or payable under the affected SOW. This enhanced cap applies collectively to all claims arising from the same engagement and replaces the general cap in Section 13.2 for claims within its scope. It does not create a separate cap for each claim or incident.

13.4 Liability that cannot be limited

Nothing in this DPA excludes or limits liability to the extent such exclusion or limitation is prohibited by applicable law. Fraud or wilful misconduct shall not be subject to the caps in Sections 13.2 and 13.3 to the

extent such liability may not lawfully be limited. Any indemnity for regulatory fines or penalties applies only to the extent permitted by applicable law.

13.5 Client authorisation claims

The Client shall be responsible for a third-party claim to the extent directly caused by the Client's material breach of its warranties concerning testing authority in Section 2.4, subject to the Services Agreement and applicable law. A party seeking indemnity shall notify the other promptly, provide reasonable cooperation and allow the indemnifying party to control the defence and settlement. No settlement may impose an admission, non-monetary obligation or continuing restriction on the other party without its prior written consent. No indemnity applies to loss caused by the indemnified party's own breach, negligence, wilful misconduct or activity outside the authorised scope.

13.6 Liability terms must be consistent

The Services Agreement must expressly identify the liability caps and exceptions that apply. A different cap replaces Sections 13.2 or 13.3 only where the written agreement specifically identifies the clause being replaced and states the replacement terms. General liability wording elsewhere does not silently alter these caps.

14. Suspension, termination and survival

14.1 Suspension

Trixent may suspend affected processing or testing where reasonably necessary to prevent unlawful processing, address a serious security risk, respond to an invalid instruction, comply with a binding legal requirement, or where required authorisation is missing or has been withdrawn. Trixent shall notify the Client promptly, where legally permitted, and describe the issue and steps needed to resume safely.

14.2 Termination

Either party may suspend or terminate the affected Services in accordance with the Services Agreement if the other materially breaches this DPA and does not remedy the breach within the applicable cure period. Where lawful processing or required authorisation cannot be restored, the parties shall follow the termination and transition provisions of the Services Agreement.

14.3 Obligations that continue

Termination does not remove obligations concerning confidentiality, incident cooperation, lawful retention, return and deletion, liability, audit rights or dispute resolution to the extent needed to give them effect. Trixent shall not continue processing Client Personal Data after the relevant Services end except as permitted under this DPA, the Client's lawful instructions or applicable law.

15. Notices and operational contacts

15.1 Contract notices

Contractual notices shall be sent to the notice addresses and contacts stated in the executed Services Agreement. The parties shall keep those details current and notify each other of changes in accordance with the Services Agreement.

15.2 Incident and emergency contacts

Security-incident notifications under Section 9 shall be sent to the designated Client incident contact and Trixent incident contact specified in the RoE or other engagement document expressly incorporated into the Services Agreement. The RoE shall also identify the emergency testing contacts and the method for requesting an immediate stop to testing. These contacts must be verified and capable of supporting the notification and escalation commitments in this DPA.

15.3 No single unmonitored route

A party shall not rely solely on a mailbox that is not monitored during the agreed response window where doing so would prevent it from meeting its obligations. Contact details may be kept in the secure engagement documentation rather than repeated in the body of this DPA.

16. How the contract documents work together

16.1 Governing order by subject

The documents for an engagement serve different purposes. The parties shall apply them as follows:

Mandatory law and transfer instruments: Mandatory law and any required international-transfer instrument prevail to the extent they govern the issue or transfer in question.

DPA: This DPA governs processing of Client Personal Data and the specific confidentiality, security, incident, use and deletion obligations it expressly covers.

Rules of Engagement: The RoE governs technical testing scope, targets, windows, permitted methods, exclusions and operational instructions. It does not expand processing permissions under this DPA.

Statement of Work: The SOW governs the service scope, deliverables, timeline, fees, retests and engagement-specific details. It modifies a DPA obligation only when it expressly identifies the DPA clause and the agreed variation.

Master Services Agreement: The MSA governs general commercial terms, subject to the specific provisions of this DPA and any expressly agreed variation.

Non-Disclosure Agreement: The NDA may add confidentiality protection. It does not reduce the use restrictions, security measures, incident notification or deletion protections expressly provided by this DPA. If a conflict remains, the parties must resolve it in writing before the affected processing begins.

16.2 No silent amendment

A general reference to another document, a public policy, a website statement or a later DPA version does not silently amend a signed DPA obligation. Any intended change must identify the applicable clause and be agreed through the written amendment process.

16.3 Governing law and disputes

The governing law, dispute-resolution, venue or arbitral-seat provisions in the executed Services Agreement apply to this DPA. The Services Agreement must be executed and must identify this DPA by version and date before processing begins. This DPA is intended to be incorporated into the Services Agreement and is not intended to operate as a standalone agreement.

17. Amendments and general terms

17.1 Amendments

Publishing a newer version of this DPA does not amend a version already incorporated into a signed Services Agreement. Amendments must follow the written amendment process in the Services Agreement or another written process agreed by both parties.

17.2 Changes in law or processing

The parties shall cooperate in good faith to update this DPA where a change in Applicable Data Protection Law or the actual processing materially requires it. An amendment shall identify the new version and effective date and shall not silently reduce protection for an existing engagement.

17.3 Severability

If a provision is held invalid or unenforceable, the remaining provisions continue to the extent they can operate consistently with the parties' intentions and applicable law. The parties shall seek to replace an unenforceable provision with a lawful provision that most closely achieves its original purpose.

17.4 No waiver

A failure or delay in enforcing a provision is not a waiver unless the waiver is confirmed in writing by the party granting it.

17.5 Records of the agreement

Each party shall retain the executed Services Agreement, this exact DPA version and the incorporated schedules. Where a Sub-processor Register or transfer instrument is incorporated, the parties shall retain the version and date used for the relevant engagement.

Annex A — Processing description

This Annex describes the standard processing associated with Trixent's cybersecurity assessment services. The SOW must state any material deviation or additional category relevant to the engagement. It must not rely on the standard description where the actual processing differs.

A.1 Subject matter

Processing of personal data encountered or otherwise handled in providing authorised cybersecurity assessment, vulnerability assessment, penetration testing, source-code review, retesting, reporting and related services described in the SOW.

A.2 Duration

For the term of the applicable Services Agreement and the relevant engagement, followed by the return, deletion and limited retention periods in Section 11 and any lawful retention period or express written variation agreed in the SOW.

A.3 Nature and purpose

Accessing, observing, minimising, collecting where necessary, analysing, documenting, reporting on and deleting personal data to identify and validate security weaknesses in systems that the Client owns or is authorised to test. Processing is limited to the authorised Services and applicable instructions.

A.4 Categories of data subjects

As applicable to the systems within scope: the Client's employees, contractors, administrators and authorised users; customers and end users whose information is present in those systems; and other individuals whose information is incidentally encountered during authorised testing.

A.5 Categories of personal data

As reasonably necessary for the Services and to the extent present in in-scope systems: names and contact details, user identifiers, test-account information, authentication records encountered during testing, logs, requests and responses, security telemetry, screenshots, captures and data included in vulnerability findings or reports. Trixent does not require access to special-category or similarly sensitive personal data by design. If such information may be encountered, the SOW must document the relevant restrictions and additional safeguards before testing begins.

A.6 Processing instructions and restrictions

The authorised assets, testing windows, permitted techniques, exclusions, emergency contacts, report recipients and any specific data restrictions are defined in the executed SOW and RoE. Trixent shall not expand the processing or testing scope on the basis of this Annex alone.

A.7 Retention

The retention categories and defaults in Section 11 apply unless a permitted, expressly documented engagement-specific variation identifies the precise data category, period and reason. No generic statement authorises indefinite retention.

Annex B — Sub-processor register requirements

The approved Sub-processor Register is an engagement-specific schedule incorporated into this DPA by an explicit reference to its version and date in the Services Agreement or SOW. It must be provided to the Client before any Sub-processor processes Client Personal Data.

What the Register must identify

- The provider's full legal name and service or processing role.
- The categories of Client Personal Data the provider may process and the purpose of that processing.
- The countries or regions where data is stored, backed up or remotely accessed.
- Any onward transfer, applicable transfer mechanism and material location restriction.
- Whether the provider is approved for any specific contingency use.

Approval rule

Only providers expressly listed in the Register incorporated for the engagement are authorised to process Client Personal Data. A provider is not authorised merely because it appears in a public policy, internal systems inventory, generic template or another client's Register.

Where no Sub-processor is authorised

If no Sub-processor is authorised for the engagement, the incorporated Register must expressly state: "No Sub-processors are authorised to process Client Personal Data for this engagement." A missing or blank Register does not constitute approval.

Changes to the Register

Changes are subject to Section 7, including the 30-day prior written notice period and the Client's right to object on reasonable data-protection grounds. The parties shall retain the version supplied for the engagement and any written notices of later changes.

Annex C — Technical and organisational security measures

The following measures are the security baseline required for systems, personnel and providers used to deliver the Services. They are contractual requirements. Trixent must implement them for the relevant engagement and maintain supporting operational evidence. No certification or technical capability is implied unless expressly and accurately identified elsewhere in a verified agreement.

C.1 Governance and personnel

Personnel with access to Engagement Data are bound by confidentiality obligations before access and receive security and data-handling instructions appropriate to their roles.

A named engagement lead is responsible for scope, conduct, client communication and delivery. A backup contact or coverage procedure is identified for longer or operationally sensitive engagements.

Security and data-protection procedures are reviewed periodically and when a material change affects the processing.

C.2 Identity and access control

- Use individual named accounts and least-privilege permissions; shared accounts are not used for routine individual work.
- Require multi-factor authentication for accounts accessing Engagement Data and phishing-resistant MFA for privileged access where supported and appropriate.

- Review access when personnel join, change roles or leave an engagement; remove or adjust access no later than one business day after the change.
- Protect recovery methods, administrator credentials and secrets from unauthorised access.

C.3 Encryption and key management

- Encrypt Engagement Data at rest using AES-256 or equivalent-strength encryption appropriate to the data and risk, including applicable workstations, storage systems and backups.
- Enable full-disk encryption on devices that store persistent copies of Engagement Data.
- Protect data in transit over public or otherwise untrusted networks using TLS 1.2 or higher with a secure configuration; prefer TLS 1.3 where supported and do not use SSL or TLS 1.0/1.1 for such transfers.
- Restrict access to encryption keys; where technically feasible, store keys separately from the data they protect and use an established KMS, secrets manager or equivalent protected mechanism appropriate to the systems.
- Do not hard-code encryption keys or secrets into source code or commit them to version-control repositories.

C.4 Secure communication and reports

Exchange credentials, keys and sensitive documents only through the channel agreed in the RoE. Ordinary email is not treated as end-to-end encrypted unless the selected method actually provides that protection.

If a credential is received through an unapproved channel, restrict access, notify the Client promptly, treat the credential as exposed and request rotation or replacement. Delete the unsafe copy when it is safe and lawful to do so.

Deliver reports only to recipients authorised in the RoE or approved through the written change-control process. Use an encrypted channel with access controls and an expiry date where supported. If expiry is unavailable, apply and document an appropriate alternative access-revocation safeguard before delivery.

Check the intended recipient against the RoE before delivery and perform a second check for sensitive reports. Mark drafts confidential and redact secrets from screenshots unless an approved, documented exception is necessary to substantiate a finding.

C.5 Devices and engagement separation

Use devices with access controls, screen locking, current security updates and endpoint protection appropriate to the operating system and risk.

Maintain a separate, encrypted and access-controlled workspace for each engagement.

Do not store Engagement Data on publicly accessible website infrastructure or work on it from shared or public computers.

Configure testing infrastructure to reduce unintended persistence and cross-engagement exposure. Remove temporary artefacts and testing changes when no longer required, subject to the RoE and Section 11.

C.6 Logging and incident handling

Maintain appropriate records of engagement activity, including testing source addresses and timing where relevant to client correlation.

Protect logs against unauthorised access or alteration and apply the retention period required by the engagement and applicable law.

Maintain a documented route to receive, escalate and respond to suspected incidents outside ordinary business hours so the 24-hour notification commitment in Section 9 can be met.

Preserve incident evidence reasonably necessary for investigation while limiting collection and access.

C.7 Backups and recovery

Encrypt backups containing Engagement Data and restrict access to authorised personnel and systems.

Delete backup and archival copies through a documented lifecycle within 30 days after deletion from active systems.

Do not use a storage or backup system for Engagement Data if it cannot meet the agreed deletion period, unless a lawful, written variation is agreed before processing begins.

If a backup is restored for disaster recovery or legal compliance, reapply the applicable deletion instructions.

C.8 External services and AI

Do not submit Engagement Data to public AI tools, public malware-analysis services, public paste sites or other unapproved online services.

Obtain the Client's prior written approval before an external AI service processes Engagement Data; document the provider, purpose, information, location and safeguards in the approved Register or incorporated written approval.

Do not allow an approved external AI provider to train on Client material or use it for unrelated purposes.

Use anonymisation only where the result does not identify the Client or an individual by means reasonably likely to be used; pseudonymisation alone is not anonymisation.

C.9 Control exceptions

A material deviation from this Annex must be documented, risk-assessed and addressed through appropriate safeguards before the affected processing begins. Where the deviation materially reduces the agreed protection, it requires prior written agreement by authorised representatives and cannot waive a mandatory legal requirement. If an adequate safeguard cannot be implemented, the affected system or processing must not be used.

Incorporation and version

This DPA is binding only when expressly incorporated by version and date into the executed Services Agreement between the parties. Its schedules form part of the agreement only when incorporated in accordance with its terms. Publishing a later version does not amend this version for an existing engagement.

End of Data Processing Agreement v1.8 · Effective 2026-10-20