Xenmark Data Processing Agreement

Version 1.4 - Last updated 24 July 2026

Processor	Xenmark AS
Registered address	Aurvågvegen 150, 6070 Tjørvåg, Norway
Organisation number	937 996 799
Privacy contact	support@xenmark.app

This DPA forms part of the Agreement and becomes binding when the Customer accepts the Agreement or otherwise accepts this DPA in writing or electronically.

1. Scope, definitions and roles

1.1 This Data Processing Agreement (DPA) forms part of the agreement under which Xenmark AS provides the Xenmark services to the Customer (Agreement). "Services" has the meaning given in the Agreement.

1.2 "Customer Personal Data" means any personal data Xenmark processes on behalf of the Customer in connection with the Services, including the categories described in Annex 1. It does not include personal data Xenmark processes solely as an independent controller under Section 1.4.

1.3 The Customer is the controller of Customer Personal Data. If the Customer acts on behalf of another controller, the Customer is a processor and Xenmark is its subprocessor. Xenmark is the processor or subprocessor, as applicable.

1.4 Xenmark acts as an independent controller for limited processing where Xenmark determines the purposes and means, including account administration, billing, fraud and abuse prevention, security administration, legal compliance and ordinary business communications. That processing is outside this DPA and is governed by Xenmark's Privacy Policy.

1.5 Stripe is used for billing and payment processing. Stripe does not host or process Customer project content for Xenmark as a subprocessor under this DPA and processes payment and related account data under its own applicable terms and data-protection roles.

1.6 "Applicable Data Protection Law" means the GDPR, the Norwegian Personal Data Act and any other data-protection law that applies to the processing under this DPA, including the UK GDPR and UK Data Protection Act 2018 where applicable.

1.7 This DPA applies for as long as Xenmark processes Customer Personal Data. The processing details in Annexes 1 to 3 form part of this DPA.

2. Instructions and Customer responsibilities

2.1 The Agreement, this DPA, the Customer's lawful use and configuration of the Services, and any additional written instruction accepted by Xenmark are the Customer's documented instructions.

2.2 Xenmark will process Customer Personal Data only on documented instructions and only as necessary to provide, secure, maintain, back up, support, export and delete data through the Services. Xenmark will not sell Customer Personal Data, use it for targeted advertising or use it for an unrelated purpose.

2.3 If applicable law requires Xenmark to process Customer Personal Data outside the Customer's instructions, Xenmark will inform the Customer before doing so unless the law prohibits that notice.

2.4 Xenmark will promptly inform the Customer if Xenmark reasonably believes an instruction infringes Applicable Data Protection Law. Xenmark may suspend the affected processing until the issue is resolved.

2.5 The Customer determines the purposes of the processing and is responsible for its instructions, lawful basis, required notices, authorised users, the accuracy and lawfulness of Customer Personal Data, and responses to data-subject requests.

2.6 Additional instructions that require a material change to the Services, unusual technical work or processing outside the agreed scope require Xenmark's prior written acceptance and may be subject to additional fees.

2.7 The Services are not designed for special-category data, biometric identification data, criminal-conviction data, medical records or similarly high-risk data. The Customer must not knowingly submit such data unless Xenmark has agreed in writing to the processing and appropriate safeguards.

3. Confidentiality and security

3.1 Xenmark will ensure that persons authorised to process Customer Personal Data are bound by confidentiality and receive access only where necessary for their duties. The confidentiality obligation continues after their access ends.

3.2 Xenmark will maintain technical and organisational measures appropriate to the nature and risk of the processing. The current minimum measures are described in Annex 2.

3.3 Xenmark may update individual security measures where the overall level of protection is not materially reduced.

3.4 Xenmark will limit production and administrative access to authorised persons and remove access when it is no longer required.

4. Subprocessors

4.1 The Customer gives Xenmark general written authorisation to use the subprocessors listed in Annex 3 and in the current data-processing register published at https://xenmark.app/data-processing, or a replacement legal page published by Xenmark.

4.2 Xenmark will enter into written terms with each subprocessor that impose data-protection obligations no less protective in substance than the relevant obligations in this DPA.

4.3 Xenmark remains responsible to the Customer for the performance of its subprocessors to the extent required by Applicable Data Protection Law.

4.4 Xenmark will give at least 14 days' prior electronic notice before a new subprocessor begins processing Customer Personal Data or an existing subprocessor is replaced. Notice may be given by email to the account owner, an in-product notice, or a subscribed legal or data-processing update page.

4.5 The Customer must object within 14 days after notice and must state reasonable, documented data-protection grounds. If the Customer does not object within that period, the change is authorised.

4.6 The parties will try in good faith to resolve a timely objection. If no reasonable solution is available, the Customer may terminate only the affected Services before the change takes effect, subject to the Agreement.

4.7 Where advance notice is not reasonably possible because of an urgent security, legal or service-continuity need, Xenmark may make the change first and will give notice as soon as reasonably possible.

4.8 On reasonable request, Xenmark will provide information necessary to demonstrate the subprocessor safeguards. Confidential, security-sensitive or commercially sensitive information may be redacted.

5. International transfers

5.1 Xenmark is established in Norway, within the EEA. A transfer from an EEA customer to Xenmark in Norway is not a transfer outside the EEA. Norway is also covered by the United Kingdom's adequacy regulations, so a transfer from the UK to Xenmark does not require a separate UK transfer instrument solely because Xenmark is located in Norway.

5.2 If Xenmark or a subprocessor transfers Customer Personal Data to a country that is not covered by an applicable adequacy decision or regulation, Xenmark will ensure that a lawful transfer mechanism and any required supplementary safeguards apply.

5.3 The transfer mechanisms in Xenmark's contracts with its subprocessors apply to the relevant downstream transfers. A separate transfer instrument between the Customer and Xenmark will be completed only where Applicable Data Protection Law requires it for a direct transfer.

6. Assistance and personal-data breaches

6.1 Taking into account the nature of the processing, Xenmark will use appropriate technical and organisational measures to assist the Customer with data-subject rights requests where reasonably possible.

6.2 If Xenmark receives a request directly from a data subject concerning Customer Personal Data, Xenmark will notify the Customer without undue delay and will not respond substantively except on the Customer's instruction or where required by law.

6.3 Taking into account the nature of the processing and information available to Xenmark, Xenmark will provide reasonable assistance with the Customer's applicable security, breach-notification, impact-assessment and supervisory-authority obligations.

6.4 Assistance requiring material work outside ordinary service and support may be charged at reasonable rates agreed in advance, except to the extent charging is prohibited by Applicable Data Protection Law.

6.5 Xenmark will notify the Customer without undue delay after becoming aware of a personal-data breach affecting Customer Personal Data.

6.6 To the extent known, the notice will describe the nature of the breach, the categories and approximate number of affected data subjects and records, likely consequences, measures taken or proposed, and a contact point. Information may be provided in stages as it becomes available.

6.7 Xenmark will take reasonable steps to contain, investigate and remedy the breach and will provide information reasonably required for the Customer's legally required notifications.

7. Export, account deletion and end of processing

7.1 The parties choose deletion, rather than post-termination return, as the default action when the processing Services end. Before deletion begins, the Customer may retrieve Customer Data using the export or archive functions then available in the Services.

7.2 Project export or archive functions are the intended method for retrieving project content. A separate account-level personal-data export may provide structured records and metadata and may not include the binary bytes of drawings, revisions or attachments.

7.3 The Customer must complete any required export before confirming account deletion or before asking Xenmark to delete the account. Xenmark does not provide a guaranteed post-termination or post-confirmation retrieval window.

7.4 When account deletion is confirmed, the account is locked and permanent deletion is scheduled approximately 24 hours after confirmation. Projects owned by that account are placed in a read-only account-deletion state and are then deleted with their drawings, revisions, attachments, comments, replies, pins and related project records. Completion may occur after the 24-hour point where an operational retry is required.

7.5 For this deletion workflow, the account recorded in the Services as the project owner controls the project lifecycle. Project Manager, Editor and Participant roles do not preserve the project, transfer ownership or prevent deletion. Deletion of the recorded owner account therefore deletes the entire owned project even if collaborators remain or the recorded owner is no longer an active project member. Before an owner account is deleted, the Customer must export any required project data and notify affected collaborators. As a supplemental measure, Xenmark's current workflow sends an in-product notification and an email to other project members when deletion of the owner account is confirmed, but Xenmark does not guarantee successful delivery or receipt of those notices in every case.

7.6 If a non-owner account is deleted, that user is removed from projects it does not own and identifying references in retained project content are removed or anonymised where supported. The project and its content remain under the project owner. Attachments or other contributions may remain as project content after the uploader or author reference has been removed.

7.7 Residual copies in backup and subprocessor systems are isolated from ordinary use and are deleted or overwritten through the applicable backup and provider deletion cycles. Because backup copies are not individually addressable in the same way as active data, their removal may occur after active-system deletion. No fixed backup-deletion period applies unless expressly agreed in an order form. If a backup is restored, the same deletion instruction will be reapplied.

7.8 Xenmark may retain limited personal data where required by law or necessary to establish, exercise or defend legal claims. Such data will be protected and processed only for that purpose.

7.9 On reasonable request, Xenmark will provide available confirmation that the applicable active-system deletion process has completed, subject to lawful retention and the technical limits of backup systems.

8. Compliance information, audits and inspections

8.1 Xenmark will make available information reasonably necessary to demonstrate compliance with this DPA and Applicable Data Protection Law.

8.2 The parties will first use available policies, security summaries, subprocessor documentation, compliance reports and remote meetings. Xenmark will provide its standard compliance materials without charge.

8.3 The Customer or an independent auditor appointed by the Customer may conduct one audit in any 12-month period. Additional audits are permitted where required by a supervisory authority, following a material personal-data breach, or where the Customer has reasonable evidence of material non-compliance.

8.4 An on-site inspection may be used only where remote evidence is insufficient to meet a legal requirement or investigate credible material non-compliance. It must be conducted on at least 30 days' prior notice during normal business hours and ordinarily must not exceed two business days.

8.5 Audits must be limited to Customer Personal Data and Xenmark's obligations under this DPA, avoid unnecessary disruption, and must not provide access to another customer's data, source code, vulnerability details, production credentials or systems unless separately agreed or required by a supervisory authority.

8.6 The auditor must be independent, appropriately qualified, not a competitor of Xenmark and bound by confidentiality.

8.7 The Customer bears its own audit costs and Xenmark's reasonable costs for customer-specific audit support beyond the standard materials described in Section 8.2, except where Applicable Data Protection Law prohibits such cost allocation.

9. Term, precedence, changes and third-party rights

9.1 This DPA remains in force for as long as Xenmark processes Customer Personal Data.

9.2 If Xenmark materially fails to provide the data-protection guarantees required by Applicable Data Protection Law, the Customer may give written notice describing the deficiency. Xenmark will have 30 days to cure it. The Customer may terminate the affected Services if the material deficiency remains uncured after that period. Immediate suspension or termination applies only where required by law, a supervisory authority or a continuing material risk to data subjects.

9.3 For a conflict concerning Customer Personal Data, the order of precedence is: mandatory law and an applicable transfer instrument; this DPA; an applicable order form; and then the remaining Agreement. Commercial terms are unaffected unless the conflict concerns data processing.

9.4 The liability limits and governing-law provisions in the Agreement apply to this DPA to the extent permitted by law. If the Agreement contains no governing-law provision, Norwegian law applies and the courts of Norway have jurisdiction, without limiting mandatory rights of data subjects or supervisory authorities.

9.5 Xenmark may update this DPA to reflect changes in law, regulatory guidance, subprocessors or the Services, but will not materially reduce the protection of Customer Personal Data during an active subscription without the Customer's agreement. Xenmark will give prior notice of material changes where reasonably possible.

9.6 This DPA does not create contractual rights for any third party, including data subjects, except where such rights are mandatory under Applicable Data Protection Law or an applicable transfer instrument.

9.7 Notices and requests under this DPA must be sent to support@xenmark.app or a replacement privacy contact published by Xenmark.

Annex 1 - Details of processing

Processing detail	Description
Subject matter	Provision of the hosted Xenmark project and drawing collaboration Services, including project workspaces, drawings, attachments, comments, annotations, invitations, access permissions, notifications, backups, project export/archive, account-data export, account deletion, anonymisation of non-owner contributions, support and security.
Duration	For the active term of the Services and until the applicable deletion process described in Section 7 is complete.

Processing detail	Description
Nature of processing	Collection, receipt, transmission, storage, organisation, retrieval, display, access control, backup, restoration, archive generation, export, anonymisation, support, troubleshooting and deletion.
Purposes	To provide, secure, maintain, back up, support, export and delete data through the Services according to the Customer's documented instructions.
Categories of data subjects	Customer administrators and authorised users; Customer employees, contractors and representatives; invited collaborators and external project participants; notification recipients; and persons identified or depicted in Customer-uploaded content.
Types of personal data	Names; business email addresses; user and account identifiers; organisation, role and permission information; invitation and notification metadata; comments, annotations, activity records and timestamps; file names and object metadata; drawings, documents, images and attachments; personal data included by the Customer in project content; and, to the extent processed on the Customer's behalf, IP address, session, access, browser/device and security-event data generated through use of the Services.
Excluded independent-controller data	Personal data processed solely by Xenmark for the purposes described in Section 1.4 is outside this DPA.
Special categories	Not intentionally required or expected. Processing requires prior written agreement and appropriate safeguards.
Frequency	Continuous or intermittent according to the Customer's use of the Services.
Instructions	The instructions described in Section 2.1.

Annex 2 - Minimum technical and organisational measures

Access and separation: Authenticated access, role and permission controls, least-privilege administration and controls designed to separate customer data.

Encryption and credentials: TLS-based encryption in transit, provider-supported encryption at rest, and protected storage of secrets and privileged credentials.

Infrastructure and development: Network and application-security controls, restricted storage resources, provider-managed physical security, source control, review and risk-appropriate testing.

Logging and monitoring: Operational and security logging, monitoring of material failures and alerts for backup or security-relevant conditions.

Incident response: Procedures for triage, containment, investigation, remediation, documentation and customer notification.

Backup and recovery: Separate backup storage, backup-status verification, restricted restore access, documented restore procedures, and monitoring for backup and restore-drill status. Restore tests are manual unless Xenmark states otherwise.

Deletion and anonymisation: A confirmed-account-deletion workflow scheduled on an approximately 24-hour clock, deletion of projects owned by the deleting account, removal or anonymisation of supported identity references in non-owned projects, and deletion or overwrite of residual backup copies through applicable retention cycles.

Vendor management: Risk-based review, written data-processing terms and transfer safeguards for authorised subprocessors.

Annex 3 - Authorised subprocessors and other external services

A. Authorised subprocessors

The provider-dashboard configuration is authoritative for the current production location. Exact configured regions are available on reasonable request. No fixed data-residency commitment applies unless stated in an order form.

Subprocessor	Purpose	Customer Personal Data	Current processing/storage information	Transfer safeguards
Supabase, Inc.	Database, authentication and backend services	User identity and account data; project metadata; permissions; comments, annotations, activity and security data	The configured production region is maintained in Xenmark's Supabase account and is available on request. No fixed residency commitment applies unless agreed in writing.	Supabase DPA; adequacy and/or Standard Contractual Clauses and supplementary safeguards where applicable
Cloudflare, Inc.	Application delivery and hosting components; network security; Workers; R2 object storage	IP addresses and request metadata; session and security data; drawings, attachments and related object metadata	Global edge processing. The configured R2 location or jurisdiction is maintained in Xenmark's Cloudflare account and is available on request. No fixed residency commitment applies unless agreed in writing.	Cloudflare DPA; adequacy, Data Privacy Framework and/or Standard Contractual Clauses with supplementary safeguards where applicable
Backblaze, Inc.	Independent backup storage for customer files	Backup copies of drawings, attachments and related identifiers and metadata	The configured B2 bucket region is maintained in Xenmark's Backblaze account and is available on request. No fixed residency commitment applies unless agreed in writing.	Backblaze DPA; adequacy and/or Standard Contractual Clauses with supplementary safeguards where applicable
Plus Five Five, Inc. d/b/a Resend	Transactional email delivery	Recipient email address; name where included; message metadata and transactional message content	United States and other locations described in Resend's current DPA and subprocessor documentation.	Resend DPA; Data Privacy Framework and/or Standard Contractual Clauses with supplementary safeguards where applicable

B. Other external services disclosed for transparency

The following current services are not authorised to receive Customer project content under this DPA. They may receive limited payment, account or network-request data directly under their own terms. Their use must also be described in Xenmark's Privacy Policy.

Service	Purpose	Data and limitation
Stripe	Billing and payment processing	Account email, billing, subscription and payment data under Stripe's own terms. No Customer project content is authorised to be sent to Stripe.
Google Fonts	Static web-font delivery	A user's browser may send IP address and ordinary request metadata to Google when fonts are loaded. No Customer project content is authorised to be sent.
UNPKG public CDN	Runtime delivery of the pdf-lib JavaScript library	A user's browser may send IP address and ordinary request metadata when the library is loaded. No Customer project content is authorised to be sent.

Location and service changes are handled under Section 4 where they concern an authorised subprocessor. This Annex does not authorise any provider to receive Customer project content beyond the purposes stated above. Electronic acceptance: no separate signature is required where this DPA is incorporated into and accepted with the Agreement; the parties may sign a separate copy where required for procurement purposes.