

Data Processing Addendum

This Data Processing Addendum (DPA) forms part of the agreement and applicable Order Form between Systemslab and Customer for UXM and related services (Agreement). It governs Customer Personal Data processed by Systemslab on Customer's behalf. It takes effect with the Agreement unless the parties agree another effective date.

Annex I describes the processing. Annex II identifies the security measures. The incorporated Subprocessor Schedule is Annex III. Annex IV supplies the terms for transfers that require contractual safeguards. Mandatory transfer terms prevail over this DPA; this DPA prevails over other Agreement terms concerning Customer Personal Data. Negotiated changes follow the Agreement's express amendment requirements, including Subscription Agreement Section 30.6 where applicable.

1 Definitions

Applicable Data Protection Laws means the privacy and data-protection laws applicable to the processing, including the EU GDPR and supplementary national law, UK GDPR and Data Protection Act 2018, Swiss FADP, applicable electronic-communications laws and US privacy laws, including CCPA/CPRA, where relevant, as amended or replaced. Personal Data, controller, processor and related terms have their statutory meanings.

Customer Personal Data means Personal Data processed by Systemslab on Customer's behalf when providing the agreed software, SaaS, support, consulting or related services (Offerings). A Personal Data Breach is accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to that data. A Subprocessor is a separate third party, including an affiliate, engaged to process that data for Customer. A Restricted Transfer requires an approved mechanism under Applicable Data Protection Laws. SCCs means the European Commission's international-transfer clauses in Decision (EU) 2021/914. UK Addendum means the ICO's International Data Transfer Addendum to those SCCs, as amended or replaced.

2 Roles and instructions

Customer acts as controller and Systemslab as processor; if Customer is a processor for another controller, Systemslab acts as subprocessor. Systemslab acts as service provider, contractor or processor under applicable US privacy laws. This DPA applies only to the processing Systemslab actually performs on Customer's behalf.

Systemslab processes Customer Personal Data only on documented instructions to provide the agreed Offerings or as required by law. The Agreement, Order Forms, this DPA and Customer's lawful configuration and use constitute those instructions. Systemslab informs Customer before legally required processing unless prohibited by law, and promptly informs Customer if an instruction appears to infringe Applicable Data Protection Laws.

Customer is responsible for its lawful collection and use, required notices and legal bases, lawful instructions, service suitability and Customer-controlled configurations. Special-category or other unusually sensitive data is not required for standard use and must not intentionally be supplied outside the agreed lawful scope. Any expressly agreed sensitive-data processing and additional safeguards must be documented.

3 Confidentiality and security

Systemslab limits access to authorised personnel who need it for their duties and are bound by confidentiality. It maintains technical and organisational measures appropriate to the processing risks, as described in Annex II and the incorporated Information Security Addendum. Updates must not materially reduce overall protection or an express commitment. Customer secures its own systems, credentials, devices, networks and configurations.

4 Personal Data Breaches

Systemslab notifies Customer without undue delay after becoming aware of a Personal Data Breach. The notice includes available information about its nature, affected data and individuals (including approximate numbers where known), likely consequences, mitigation measures and a follow-up contact. Information may follow in phases without undue further delay; the initial notice must not await complete information or a completed root-cause investigation.

Systemslab investigates, contains and mitigates the breach, takes appropriate corrective action and reasonably cooperates with Customer's notification and regulatory obligations. It sends notices to Customer's designated security contact or, if none, its primary technical contact. Notification is not an admission of fault or liability.

5 Subprocessors

5.1 Authorisation. Customer gives general written authorisation for Subprocessors in the Schedule (Annex III) incorporated through the Customer Agreement and changes under this Section. Systemslab makes the applicable Schedule available or supplies it before Customer acceptance. An accessible online list may be used if agreed. The list identifies the legal entity, service, nature of processing and processing locations, directly or through identified provider location information. Relevant identity, contact and location information is made available to Customer.

5.2 Changes. Systemslab gives Customer's designated privacy or legal contact at least 30 days' advance email notice before an added or replacement Subprocessor begins processing. The notice identifies the supplier, processing, countries and intended start date, subject to the objection process and mandatory authorisation and transfer rules.

5.3 Protection. Systemslab contracts in writing with each Subprocessor for the same relevant data-protection obligations, including confidentiality, security, breach handling, assistance, return/deletion and transfer safeguards. Further subprocessing remains subject to applicable authorisation and written obligations. Systemslab remains responsible to Customer for its Subprocessors' performance under Applicable Data Protection Laws, subject to Section 13 and mandatory transfer terms.

5.4 Objections. Customer may object on reasonable data-protection grounds within 30 days of notice by explaining the grounds to legal@uxmapp.com. Without a timely objection, the change is authorised. Systemslab uses reasonable efforts to provide an alternative arrangement or commercially reasonable service/configuration change addressing the objection without unreasonably burdening Customer. If none is available within 30 days after objection, Customer may terminate only the affected service that cannot be supplied without the disputed Subprocessor.

While resolving an objection, Systemslab may suspend affected processing as needed to comply with law or authorisation requirements; unaffected services may continue. Amounts properly due before termination remain payable. This termination does not itself create a prepaid-fee refund, additional early-termination charge or acceleration of future fees. Refunds or fee cancellation required elsewhere in the Agreement or by law remain effective and follow Subscription Agreement Section 11.4 where applicable. Rights for breach and non-excludable rights are preserved.

6 Data location and international transfers

6.1 Hosting and access. The standard UXM SaaS infrastructure is Google Compute Engine through Google Cloud. The Customer selects the hosting region. The selected region is recorded in the Order Form. UXM application data, all replicas, backups and application workloads remain within that region. Systemslab shall not replicate UXM application data or backups outside the selected region.

Customer authorises necessary remote access by Systemslab's authorised employees from outside the hosting region to operate, secure, maintain and support the Offerings, subject to documented instructions, confidentiality, Annex II, the Information Security Addendum and applicable law, including transfer safeguards where required. Systemslab remains responsible for its employees. Remote access does not change the selected hosting region.

Google infrastructure maintenance and support, and separate processing of support communications, documentation or email alerts by authorised suppliers, are governed by Sections 5–6 and Annex III. Google processing is also subject to the Google Cloud Data Processing Addendum accepted by Systemslab. Relevant provider location information and operational-access information are reasonably available to Customer. A selected hosting region does not represent a promise that every supplier operation or support activity occurs there.

6.2 EEA transfers. Systemslab uses an applicable adequacy decision or other lawful mechanism. Where a GDPR Restricted Transfer from Customer to Systemslab requires SCCs, the SCCs are incorporated with Module Two for controller-to-processor transfers or Module Three for processor-to-processor transfers, completed as set out in Annex IV.

6.3 UK transfers. Where required for a UK Restricted Transfer using the SCCs, the UK Addendum is incorporated and completed as described in Annex IV.

6.4 Swiss transfers. Transfers subject to the Swiss FADP use a recognised mechanism; where SCCs apply, the Swiss adaptations in Annex IV apply.

6.5 Assessment and safeguards. The parties reasonably cooperate with required transfer assessments. Systemslab supplies reasonably available information about processing, suppliers and security, and implements supplementary safeguards where required. Systemslab ensures its onward Restricted Transfers to Subprocessors are covered by the applicable mechanism before access or disclosure.

6.6 Alternative mechanism. Systemslab may use a lawful alternative transfer mechanism on reasonable notice, provided protection is not materially reduced.

7 Data subject rights

Customer is responsible for answering individuals' requests. Taking account of the processing, Systemslab provides reasonable assistance through appropriate technical and organisational measures for access, correction, erasure, restriction, portability, objection and other applicable rights. It refers direct requests to Customer or notifies Customer where reasonably possible and does not independently answer their substance unless legally required.

8 Compliance assistance

Taking account of the processing and information available, Systemslab reasonably assists Customer with security, breach notifications, impact assessments, supervisory-authority consultations and other statutory processor-assistance duties. Customer determines whether an assessment or consultation is required.

9 Public authority requests

Unless prohibited by law, Systemslab promptly notifies Customer of binding authority requests for Customer Personal Data, supplies available details, seeks redirection to Customer where appropriate and limits disclosure to what is legally required. Where lawful and reasonably appropriate, it challenges requests considered unlawful, disproportionate or inconsistent with transfer safeguards.

10 Return and deletion

At Customer's written choice, Systemslab returns Customer Personal Data then held and deletes remaining copies, or deletes the data and copies. Return instructions received by expiry or termination of the applicable Offering are fulfilled within 30 calendar days after that date; those received during retrieval, within 30 calendar days of receipt, subject to shorter mandatory deadlines. Return uses a commonly used structured format, machine-readable where required; meaningful tabular data uses CSV.

The Agreement governs retrieval and switching, including retrieval after transition. A timely request preserves its return copy until delivery, subject to mandatory deadlines, without extending production use.

Absent return instructions, Systemslab deletes active copies without undue delay after retrieval, or earlier on lawful instructions. Following return, remaining active copies are deleted without undue delay once return and retrieval are complete, unless lawfully instructed to delete earlier.

Where law and the Agreement permit, protected automated routine backups expire under Systemslab's documented retention/deletion policy. It must set appropriate finite retention periods and deletion cycles; relevant information is available on request. Backups remain confidential, secure and beyond ordinary use. On recovery, deletion instructions are reapplied before ordinary processing resumes. A routine cycle cannot extend an agreed or mandatory deletion deadline.

Legally required retention is limited to the necessary data and period. Systemslab imposes corresponding return/deletion duties on Subprocessors; supplier terms do not override mandatory rights. On reasonable request, Systemslab confirms deletion status and any permitted backup/legal retention and its basis or cycle.

11 Compliance information and audits

Systemslab makes available information necessary to demonstrate compliance, including relevant control descriptions, available independent reports, questionnaires, policies and Subprocessor information. Customer or its appointed auditor may audit and inspect compliance where reasonably necessary under Applicable Data Protection Laws.

Routine audits ordinarily occur no more than once in 12 months. This does not restrict additional audits following a material breach or compliance concern, an authority request or mandatory requirements. Audits use reasonable written notice, normal business hours, confidentiality and security safeguards, and avoid unreasonable disruption. Available independent reports and documentation are used first where reasonably possible; insufficient documentation does not prevent a necessary further audit. Customer bears its own audit costs unless a material DPA breach is identified.

12 US privacy requirements

Where applicable, Systemslab processes data only for the specific business purposes in the Agreement and DPA, provides the statutory level of protection and does not sell data or share it for cross-context behavioural advertising except where expressly lawful and agreed by Customer. It does not retain, use or disclose data outside the direct relationship, or combine it with unrelated-source data, except as law permits. Systemslab notifies Customer if it can no longer meet applicable duties, permits reasonable statutory verification/remediation steps and passes relevant duties to Subprocessors.

13 Liability. The Agreement's exclusions and limitations apply to liability under this DPA, except where prohibited by Applicable Data Protection Laws or mandatory transfer terms. Non-excludable rights of individuals and supervisory authorities are preserved.

14 Duration. This DPA applies while Systemslab processes Customer Personal Data. Confidentiality, security, deletion, transfer and other continuing obligations survive while that data is retained.

15 Other terms. Other Agreement terms remain unchanged. Its governing law and jurisdiction apply, except where Applicable Data Protection Laws, SCCs, the UK Addendum or another mandatory mechanism require otherwise.

Annex I Processing details

Parties. Customer is the entity in the accepted Agreement or Order Form, with its stated address and designated privacy/legal contact, acting as controller or processor. Systemslab ApS, CVR 25716027, Slotsmarken 18, 2., 2970 Hørsholm, Denmark, acts as processor or subprocessor. Its privacy, legal and security-reporting contact is legal@uxmapp.com. The accepted Agreement supplies the parties’ acceptance details.

Subject matter and purpose. Providing, operating, securing, maintaining and supporting the agreed UXM services: business application usage, application performance and endpoint performance monitoring, technical issue identification, troubleshooting and remediation under Customer’s documented instructions. For on-premises deployments, this DPA covers support and other processing actually undertaken by Systemslab; it does not transfer Customer’s local infrastructure responsibilities.

Individuals. Customer employees, contractors and other authorised users of the monitored business IT environment; customer contacts requesting support or receiving configured alerts.

Data category	Agreed scope
User identifiers	Names, business usernames/user identifiers and business email addresses.
Device and login information	Hostnames, IP addresses and login information associated with business users and devices.
Application and endpoint telemetry	Application usage, application performance and endpoint performance information and metrics.
Support material	Business contact details and Customer Personal Data in customer system documentation, support messages, screenshots, diagnostic logs, attachments and recordings, as necessary for agreed support.
Configured email alerts	Recipient business email addresses, delivery metadata and Customer Personal Data within the agreed categories included in alert messages.

These categories are Personal Data to the extent linked or reasonably linkable to individuals. No additional category is authorised merely because it could be captured technically. Special-category/sensitive data is not required for standard services; any expressly agreed processing and safeguards are recorded in the Order or other written agreement.

Operations and frequency. Collection, receipt, transmission, storage, organisation, retrieval, consultation, analysis, troubleshooting, security monitoring, support and deletion as needed for the agreed services. Processing is continuous, periodic or one-off depending on configuration and service use.

Duration and retention. Processing continues for the service term and the limited return, retrieval and deletion process under Section 10, the Agreement and applicable law. Protected routine backups follow the documented retention/deletion policy, subject to mandatory erasure and switching requirements. Relevant retention information is available to Customer on request. Customer support data in Microsoft 365 is deleted following termination or expiry under the Customer Agreement and this DPA. This Annex grants no unrestricted retention right.

Locations and authority. Section 6 and Annex III identify hosting and operational processing. The competent supervisory authority follows applicable law and SCC Clause 13; Datatilsynet applies where it is the competent authority. Annex IV addresses transfer-specific particulars.

Annex II Security measures

The Systemslab Information Security Addendum available at <https://www.uxmapp.com/legal> when Customer accepts the Order, is incorporated into this Annex and must be supplied with this DPA. Its full controls, responsibilities and review/testing commitments apply. The summary below does not replace or reduce them. Measures apply to Systemslab-controlled processing, including on-premises support information; Customer-controlled infrastructure follows the agreed allocation of responsibilities.

Access and people. Individually approved accounts, least privilege, annual access reviews and prompt removal; human privileged MFA; restricted service accounts and managed credentials; controlled, logged emergency access. Equivalent restrictions apply to authorised support-provider access. Confidentiality, onboarding and annual instruction, managed-device protection/encryption and lawful screening where appropriate apply.

Encryption and protection. Secure public-network transport, encryption at rest for UXM production databases, storage and backups, restricted keys/secrets, and appropriate encryption/access controls for support repositories and exports. Coverage, responsibilities and permissible exceptions are documented. Email alert content is minimised; ordinary email is not guaranteed end-to-end encrypted.

Infrastructure and development. Appropriate network restrictions, secure configuration, malware protection, restricted source access, controlled production changes and pre-deployment testing. Vulnerability scanning, dependency review, risk-based patch/remediation processes and independent penetration testing follow documented schedules, with tracked findings and verified corrective actions.

Monitoring and incidents. Protected logs cover relevant privileged activity, authentication and material access/configuration changes. Monitoring and escalation have assigned owners and documented coverage. Incident procedures cover detection, evidence, containment, remediation, communication and lessons learned. Section 4 governs Personal Data Breach notice. No separate staffed 24/7 service is created.

Backups and continuity. Documented scope, frequency, retention, access controls and success monitoring; restore tests at least annually and after material changes where needed. Application data, replicas, backups and workloads stay in the selected region under Section 6.1. Internal recovery objectives are not guaranteed RTO/RPO unless expressly agreed; SLA commitments remain separate. Deletion obligations continue to apply to backups.

Suppliers and governance. Supplier risk/assurance review, limited-purpose access, protected physical access and hosting-provider assurance. A written security programme includes responsibility, risk assessment, control review and corrective actions, with management review at least annually and after material changes/incidents. Provider certification does not imply Systemslab certification.

Systemslab retains evidence and reasonably supports assessments under Section 11. Changes must not materially reduce overall protection or express commitments. Where SCCs require supplementary measures, those measures are documented for the relevant transfer and provided with the applicable transfer information.

Annex III Authorised Subprocessors

The Systemslab UXM Subprocessor Schedule available at <https://www.uxmapp.com/legal> when Customer accepts the Order forms Annex III. Make it available with the DPA before acceptance. Only suppliers applicable to the agreed services are authorised. Later additions or replacements follow Section 5. Supplier references do not amend Systemslab's obligations or authorise incompatible locations, retention or onward processing.

Annex IV Conditional transfer terms

This Annex applies only where contractual transfer safeguards are required. It does not treat every EU/UK service use or internal employee access as a Restricted Transfer. Systemslab's onward transfers to suppliers must be covered by their applicable transfer arrangements; the Customer–Systemslab SCCs do not automatically replace those arrangements.

EU SCCs. For a qualifying transfer from Customer (exporter) to Systemslab (importer), the unmodified SCCs in Decision (EU) 2021/914 are incorporated by reference. Module Two applies if Customer is controller; Module Three if Customer is processor. Clause 7 docking applies. Clause 9 uses Option 2, general written authorisation, with the 30-day advance notice in Section 5. The optional language in Clause 11 does not apply.

Law and courts. For Clauses 17–18, use the EU Member State law and courts specified in the accepted Order, provided third-party beneficiary rights are permitted. If none is specified, Danish law and competent Danish courts apply to the extent permitted by the SCCs. Mandatory SCC jurisdiction and individuals' rights prevail.

SCC Annexes. Annex I.A uses the parties, roles, addresses, contacts and acceptance details in DPA Annex I and the accepted Agreement/Order. Annex I.B uses the processing, frequency, duration, categories and any agreed sensitive-data safeguards in DPA Annex I. Annex I.C uses the authority determined under SCC Clause 13, with the applicable Customer establishment or representative identified in the Order where needed. Annex II uses DPA Annex II and the supplied Security Addendum. The authorised supplier list is DPA Annex III; further details needed for a particular transfer are provided with its transfer information.

UK Addendum. Where Section 6.3 applies, the ICO International Data Transfer Addendum (version B1.0, in force 21 March 2022, or its valid successor) is incorporated. Table 1 uses the exporter/importer and contact details above and the Agreement's acceptance details. Table 2 selects the SCC modules and options above. Table 3 uses the corresponding DPA Annexes. For Table 4, neither party may terminate solely under Part 2 Section 19 unless the accepted Order expressly selects an entitled party. The Addendum's mandatory clauses apply and prevail as required.

Swiss adaptations. Where the SCCs safeguard transfers under the Swiss FADP, references to GDPR include the Swiss FADP as applicable, protected individuals include those in Switzerland, and the Swiss Federal Data Protection and Information Commissioner is the competent Swiss authority. References to an EU Member State must not prevent Swiss individuals enforcing rights in Switzerland. Where a transfer is subject exclusively to Swiss law, Swiss law and competent Swiss courts apply where the relevant SCC provisions permit; otherwise the valid EU selections above remain, with mandatory Swiss rights preserved.

[EU SCCs — Decision \(EU\) 2021/914](#)

[ICO International Data Transfer Agreement and Addendum](#)