

Export and Deletion Guide

This Export and Deletion Guide is the “UXM Export Guide” referenced in SaaS Sections 20.4–20.5. It explains export, exit retrieval and deletion and forms part of the Documentation. The Subscription Agreement governs switching, fees and termination; DPA Section 10 governs Customer Personal Data. Mandatory rights and the agreed retrieval period prevail.

1 Send your request

Email legal@uxmapp.com with Customer’s name, tenant, service, authorised contact/recipient and whether you request a copy, switching or termination and erasure. Identify data/period, destination, timetable, final export and deletion instructions. For a complete export, request all exportable data and portable digital assets. Systemslab verifies authority and confirms delivery. Customer may act directly or authorise a reseller/migration provider; separate reseller approval is not required. A narrower request does not waive remaining rights.

2 Export scope and format

The export covers Customer input and output data, associated metadata and portable digital assets held for Customer, including personal and non-personal data within the Agreement and law. It depends on the purchased modules, configuration and data still lawfully held. There is no duty to recreate information already lawfully deleted before the request, without limiting preservation duties or mandatory rights.

Category	Included where held and applicable
Business users devices and logins	Names, business usernames/identifiers, business emails, hostnames, IP addresses and login information.
Application and endpoint telemetry	Application usage/performance and endpoint performance data and metrics.
Customer inputs and portable assets	Customer-supplied data and portable configurations, monitoring/alert rules, report/dashboard definitions and scripts Customer has an independent right to use.
Customer outputs and metadata	Customer-specific results, reports, scores, aggregations and alert history, with identifiers, timestamps, units, relationships and schema information needed to interpret them.
Support material	Relevant Customer Personal Data in support communications, documentation, screenshots, logs, attachments and recordings; return may be arranged separately under the DPA.

Tabular data uses CSV. Non-tabular assets use existing digital formats or appropriate structured, commonly used, machine-readable formats where required. The export identifies files, schema and formats. Software, source code, protected algorithms, trade secrets and security-sensitive internal information are excluded only as law permits. Customer outputs are not excluded merely because they are derived or labelled telemetry; exclusions must not obstruct switching.

3 Delivery and technical information

Systemslab provides secure recipient-restricted delivery, access/authentication instructions and download availability, subject to applicable transfer safeguards. A manifest and field information identify data/assets, period/cut-off, formats, schema, units/timezones, relationships, transformations, file parts and lawful exclusions. CSV headers and settings accompany the files.

Systemslab checks scope, readability and completeness. Customer checks receipt and reports problems for correction. Splitting or practical limits must not unlawfully restrict or delay export; silence does not waive rights. The parties coordinate final exports and destination mapping without guaranteeing equivalent functionality elsewhere.

Systemslab maintains an accessible, current online technical register of the relevant data structures, formats, standards, interfaces and interoperability information where law requires it. The applicable register identifies datasets/portable assets, lawful exclusions, retention horizons, available interfaces or assisted-export methods and relevant practical limits. Supply this Guide and the applicable register with the Customer terms before acceptance.

Applicable technical reference: Systemslab UXM Export Technical Reference available at <https://www.uxmapp.com/legal> when Customer accepts the Order, supplied with this Guide. Subsequent changes follow the applicable Agreement's change provisions.

4 Ordinary expiry and termination

Customer has 30 calendar days after expiry or termination to retrieve exportable data, unless law or an express agreement gives longer. Under DPA Section 10, return instructions received by the end of the service are fulfilled within 30 calendar days after that date. A request received during the retrieval period is fulfilled within 30 calendar days of receipt, subject to any shorter mandatory deadline. A timely request preserves the return copy until delivery without extending ordinary production use.

If Customer gives no return instructions, active Customer Personal Data and remaining copies are deleted without undue delay after the retrieval period, or earlier on lawful instructions. Other Customer exportable data is handled under SaaS Sections 20.4–20.5. Protected routine backups and legally required records follow Section 6 below. Customer should retrieve what it needs before requesting irreversible deletion.

5 Mandatory SaaS switching

Where the EU Data Act applies, SaaS Section 20.5 governs: no more than two months' notice, then a transition without undue delay and within 30 calendar days, subject to extensions. If technically unfeasible, Systemslab gives reasons within 14 working days and an alternative transition of no more than seven months; Customer may extend once for an appropriate period. Service ends on successful switching, or at notice end for termination/erasure without switching, with notice to Customer. Retrieval lasts 30 calendar days after transition, or longer where required or agreed. Mandatory erasure/transfer duties prevail.

During transition, Systemslab provides the required reasonable assistance, maintains contracted functions and continuity with due care, secures transfer/retrieval and identifies known continuity risks. Mandatory switching assistance, export, retrieval, erasure and associated data egress carry no separate charge. The existing subscription and remaining-term fee settlement in SaaS Section 20.5(d) and the accepted Order still apply, including mandatory reductions, agreed payment dates and no double recovery. Settlement cannot delay switching or erasure. Optional extra work requires a separate accepted SOW and cannot condition mandatory work.

6 Backups legal retention and confirmation

After successful switching and the retrieval period, Systemslab erases the relevant exportable data and digital assets as required by SaaS Section 20.5. Where retention is permitted, protected routine backups expire under the documented retention and deletion policy; the policy sets finite retention periods and deletion cycles, with relevant information available on request. Backups remain secure and beyond ordinary use. Deletion instructions are reapplied on recovery before ordinary processing resumes. Routine cycles cannot extend agreed or mandatory deletion deadlines.

Legally required retention is limited to the necessary data and period. The same applicable return/deletion duties cover authorised support and alert suppliers; their recovery cycles do not override mandatory rights. On reasonable request, Systemslab confirms deletion status and identifies any protected backup or legally retained copies and their basis or cycle. DPA protections continue until deletion.