EU DATA ACT INFORMATION NOTICE — SAFEQ CLOUD

Version: 1
Effective date: 12 September 2025
Applies to: Y Soft SAFEQ Cloud (the "SAFEQ Cloud")
Incorporation: This Notice forms part of the pre-contract information package for SAFEQ Cloud. Your **Contract** governs the service. For personal data, the **Data Processing Terms** apply.

If you are interested in the provision of SAFEQ Cloud, this Information Notice provides you with information required by Regulation (EU) 2023/2854 (the "EU Data Act"). Not defined terms used herein have the same meaning as in the EU Data Act.

Definitions used in this Notice:

Provider means Y Soft Corporation, a.s.. with its registered office at Technická 2948/13, Královo Pole, 616 00 Brno, Czech Republic, registered by the Regional Court in Brno under Section B, File 8045.
Customer means the entity that purchases the right to use SAFEQ Cloud from the Provider or through one of its resellers; for pre-contract information in this Notice, Customer refers also to the user.
Contract means the legally binding terms governing your access to and use of SAFEQ Cloud, whether entered into directly with the Provider or indirectly through an Authorized Reseller, including any order forms, statements of work, service schedules, pass-through or mandatory terms, and any documents incorporated by reference.
Authorized Reseller means a third party authorised by the Provider to resell access to SAFEQ Cloud and to pass through mandatory Provider terms, where applicable.
Data Processing Terms means the binding terms that govern the processing of personal data in connection with SAFEQ Cloud between the Customer and the Provider (or, where applicable, via an Authorized Reseller). In case of conflict concerning personal data, the Data Processing Terms prevail.
Support Portal: means a secure, web-based interface provided by the Provider through which the Customer may access helpdesk, authorized support resources, submit and manage support requests, monitor status of support request, and communicate with the Provider's support team. Available to Customer authorized users after onboarding.
SAFEQ Cloud means a related service and a data processing service that processes data generated by or in relation to connected printing/scanning products and client apps.

A) RELATED SERVICE — INFORMATION NOTICE (Art. 3)

Item required by the EU Data Act	**SAFEQ Cloud — Information**
Nature of data obtained (Product & Related Service Data)	**Operational telemetry & service events:** service health/performance, client/terminal status, sync/update status, authentication and API events, admin audit trails. **Print/scan job metadata:** owner/login identifier, job title, submission time, device/queue identifiers, pages/size, state, release events, scan destinations & delivery results. **Configuration & account data:** tenant IDs, roles/permissions, departments/cost centres, device registrations, API keys/tokens. **Document content:** Document content may be processed transiently only to provide requested features.
Format of data	Machine-readable records surfaced in the Admin UI (reports/dashboards) and via documented APIs. Exports typically available as CSV, XLSX, PDF, HTML or XML (where applicable).
Estimated volume	Varies with usage (e.g., number of users/devices and job frequency). Telemetry and audit logs are event-based; job metadata scales with submitted/processed jobs.

Item required by the EU Data Act	SAFEQ Cloud — Information
Collection frequency	Near real-time event ingestion for service operation; continuous where technically feasible, batch where appropriate for performance and cost.
How to access & retrieve data (Readily Available Data)	Admin UI exports; audit-log viewing/export; documented APIs with token-based access and granular scopes; on request, provider assistance for bulk retrieval.
Storage location	Data at rest are hosted in the EU region selected for the tenant (EU public cloud or EU sovereign option). Support access does not change data-at-rest location. See section **C.2** for jurisdictions.
Intended retention	Operates on rolling windows appropriate to feature and configuration (e.g., logs/caches). Customer-controlled retention for personal data via DPA and product settings. Backups and legal holds may extend retention as required by law.
Intended uses by Provider	Uses by the Provider will be as agreed in your Contract (and, where applicable, subject to the Data Processing Terms for personal data) and may include, to the extent applicable to SAFEQ Cloud: (a) provision of the SAFEQ Cloud; features delivery (print/scan handling, audit logging, reporting, client auto-update, etc.); (b) support, warranty/guarantee or similar services, or assessing claims by the Company or third parties; (c) monitoring and maintaining the functioning, safety and security of SAFEQ Cloud and ensuring quality control; (d) improving and further development of SAFEQ Cloud; (e) developing new products or services, including AI solutions, by the Provider or by third parties acting on its behalf, in collaboration with other parties or through special-purpose companies; (f) aggregating these data with other data or creating derived data for any lawful purpose, including making aggregated or derived datasets available to third parties, provided such datasets do not allow specific data transmitted from connected products to be identified or allow a third party to derive those data from the dataset; all without re-identification the Customer or individuals or disclose customer-level insights or trade secrets.
Disclosure to third parties	No disclosure of Readily Available Data to third parties except (i) to **Customer-designated Data Recipients** under Art. 5 on FRAND terms (see **A.2**), (ii) sub-processors listed in the current register for hosting/support, and (iii) as required by law.
Other data-processing parties	See **Sub-processor Register.**
Trade-secret holder(s)	The Provider is **not** a trade-secret holder in the data. The **Customer** is the trade-secret holder in the data it generates or provides via SAFEQ Cloud. Where third-party trade secrets are implicated, it is the Company's responsibility to identify them and apply proportionate safeguards (NDAs, secure portals, minimisation/redaction) before sharing.
Means of communication (contacting the data holder quickly & efficiently)	Support portal (available to account holders after onboarding)
How to share / stop sharing with a third party	**Start sharing:** Customer Admin requests under the Data Act via Support Portal. **Stop sharing:** use the same channel/UI to revoke access or submit a stop request.
Contract duration & termination arrangements	**Governed by your Contract.** For the effects of termination on data access/retrieval, see section **B.1** (switching & porting).

Item required by the EU Data Act	SAFEQ Cloud — Information
Complaints route (Data Act)	Without prejudice to judicial remedies, you may lodge a complaint with your national competent authority under the EU Data Act.
Identity & contact of (prospective) data holder	Y Soft Corporation, a.s. ("Provider"). Contact for Data Act requests: **Support portal**

B) DATA PROCESSING SERVICE — INFORMATION NOTICE (Arts. 25–30)

B.1 Switching & Porting Summary (Art. 26 & 29)

Topic	SAFEQ Cloud — Summary
What can be ported	Customer data (including Readily Available Data, configurations and relevant metadata) in commonly used, machine readable formats. Document content is retrieved via standard product features (e.g., job release/scan delivery) and is otherwise not retained.
Methods & formats	Admin exports (CSV/XLSX/PDF/HTML/XML where available); API retrieval; on request, provider-assisted bulk export. See the **Formats & Interfaces Register** in **B.3**.
Timeframe & transitional period	Retrieval window and reasonable assistance provided following notice of switching or contract end; erasure follows retrieval/exit subject to backup/legal-hold constraints. Minimum windows/assistance are set in your Contract.
Limitations/exclusions	Protection of third-party IP and trade secrets; security safeguards; technical limits of interfaces.

B.2 International governmental access transparency (Art. 28)

This Notice also serves as the provider's **Article 28 transparency webpage** for SAFEQ Cloud. It sets out (i) the **jurisdiction(s)** applicable to the ICT infrastructure and (ii) the **technical, organisational and legal measures** adopted to prevent unlawful international governmental access to or transfer of nonpersonal data in conflict with Union or Member State law. See section **C.2** for jurisdictions and **C.3** for Measures against unlawful international access. The **stable URL of this Notice** is listed in our contracts as required by Article 28(2).

B.3 Online register of data structures, formats & interfaces (Art. 26(b))

A public **Formats & Interfaces Register** for SAFEQ Cloud is provided via the SAFEQ Cloud Documentation Portal.

B.4 Fees, early termination penalties & switching charges (Art. 29(4)–(6))

Item	Information
Standard service fees (price list)	As provided by your Authorized Reseller
Early termination penalties (if any)	No early termination penalties apply
Switching charges	No switching charges apply

B.5 Applicability notice (Art. 31(3)

Production SAFEQ Cloud environment: Chapter VI obligations **apply**.

Non-production/test/DEMO SAFEQ Cloud environment: Chapter VI obligations DO NOT apply.

C) SECURITY, SOVEREIGNTY & LOCATIONS (SUMMARY)

C.1 Security & resilience

Layered technical and organisational measures include TLS by default, role based access control and MFA options, privileged operation audit logs, backups/restore testing, vulnerability/patch management, environment separation, multitenant isolation, and secure development practices. Details and current certifications are provided in the Data Processing Terms annexes and security documentation.

C.2 Processing locations & applicable jurisdictions (transparency)

- **EU regionalised hosting:** Tenant data are hosted in the selected EU public cloud region. Jurisdiction(s): relevant EU Member State(s) of that region.
- **EU sovereign option:** Hosting in an EU sovereign cloud operated by a qualified EU provider. Jurisdiction: EU (Member State specific).
- **Support & service teams:** Y Soft Group entities may provide support from multiple countries; remote access is controlled/audited and does not change data at rest location.
- **Sub-processors:** Listed in the current **Sub-processor Register** with locations and roles.

C.3 Measures against unlawful international access (Art. 28)

- **Technical:** encrypted transport, hardened admin planes, strong authentication, tenant isolation, monitored privileged access, protected backups, secure erasure post exit.
- **Organisational:** least privilege access governance, timebound support access, confidentiality/training, vendor due diligence, trade secret handling.
- **Legal:** contractual controls with infrastructure/support providers; challenge and minimum disclosure principles for conflicting third country demands; notification where legally permitted.

F) CONTACTS

Data Act access/sharing requests: via the Support portal.

G) CHANGES TO THIS NOTICE

We may update this Notice to reflect changes in law, features or security practices. Updates to this Notice do not amend your Contract. Your contract (including switching terms under the EU Data Act) is governed by your Contract and its change mechanism.

We maintain a version history and effective dates at this stable URL.