Oktopi EU Data Portability and Switching Register

19 June 2026

This Register was last reviewed and updated on 19 June 2026

Published pursuant to Article 26 of Regulation (EU) 2023/2854 (EU Data Act)

Introduction

Oktopi Pty Ltd (ACN 672 021 911) **(Oktopi, we, us)** provides cloud-based software-as-a-service solutions (Cloud Services) to customers in the life sciences and global health sector. This register is published in accordance with Article 26 of the EU Data Act (Regulation (EU) 2023/2854) and is maintained for the benefit of customers who are established in the European Union or whose Authorised Users access the Cloud Services from within the European Economic Area (EEA).

This register covers the four categories of information that Oktopi is required to make publicly available under the EU Data Act to facilitate switching and data portability. It is updated whenever there is a material change to the relevant information and reviewed in full at least annually.

Questions about this register should be directed to info@oktopi.com.

Register 1 — Switching and Porting Procedures

This register sets out the procedures available to EU Customers who wish to switch from Oktopi's Cloud Services to a different data processing services provider, or to export their data to an on-premises ICT infrastructure, in accordance with section 3 of the EU Terms of Oktopi's SaaS Framework Agreement.

1.1 How to initiate a switch

An EU Customer may initiate a switch by providing Oktopi with a written Switching Notice addressed to:

Contact	Chief Operating Officer
Email	info@oktopi.com
Postal address	L4, 627 Chapel Street, South Yarra VIC 3141, Australia

The Switching Notice must include:

- a description of the intended switch, including whether the EU Customer intends to move to a different provider or to an on-premises environment;
- the intended date of commencement of the switch; and
- where applicable, the name and relevant contact details of the destination provider of data processing services.

1.2 Transitional Period

Two calendar months after Oktopi receives a valid Switching Notice, a Transitional Period of up to 30 calendar days will commence. During the Transitional Period, Oktopi will:

- provide reasonable assistance to the EU Customer and any third parties authorised by the EU Customer to facilitate the switch;
- maintain continuity of the Cloud Services and business operations;
- provide information about any known risks to continuity of service;
- maintain a high level of security for all Exportable Data and Digital Assets during export; and
- enable export of Exportable Data and Digital Assets as described in Register 2 of this document.

The EU Customer may extend the Transitional Period once before its expiry by giving written notice to Oktopi. Where it is technically unfeasible to complete the switch within 30 calendar days, Oktopi may extend the Transitional Period by up to 6 months by giving written notice within 14 days of the Switching Notice, setting out the reasons for the extension.

1.3 Data Recovery Period

Following the end of the Transitional Period, Oktopi will provide a Data Recovery Period of at least 30 calendar days during which the EU Customer may export its Exportable Data and Digital Assets from the Cloud Services.

At the end of the Data Recovery Period, Oktopi will securely erase all Exportable Data and Digital Assets generated directly by or relating directly to the EU Customer, unless Oktopi is required to retain such data under applicable law. Oktopi will provide written certification of deletion upon request.

1.4 Available export methods and formats

Exportable Data can be exported from OktoWai and OktoPilot using the following methods:

- Exportable Data is available through an administrative export function that captures all data belonging to a single organisation and all content within it, following the tenancy hierarchy (Organisation → Workspace → Project → Task).
- This export is the customer-facing data portability and offboarding mechanism and is distinct from an individual user's data portability rights under Article 20 of the GDPR.
- The export includes personal data of the organisation's members (such as names, email addresses and audit records). EU Customers should handle that subset in accordance with their existing GDPR obligations. All other exported content comprises the organisation's own business content and operational records.

Supported export formats include a combination of JSON and CSV, depending on the data category. See Register 2 for a full list of exported files and formats.

1.5 Known restrictions and technical limitations

The following restrictions and technical limitations apply to the switching process:

- Files uploaded by Customers to the Cloud Services are not re-exported as part of the switching process, as Customers retain those files and do not require Oktopi to return them.

- The export package includes personal data (such as user profile information) that is subject to GDPR. EU Customers are responsible for handling that data in accordance with their own GDPR obligations.
- AI generated content that forms part of document creation provenance is included in the export where recorded.
- Oktopi's proprietary taxonomies and other confidential platform information are not included in the export.

Register 2 — Data Structures, Formats and Interoperability

This register describes the categories of Exportable Data and Digital Assets available to EU Customers, the data structures and formats in which they are held, and the relevant standards and open interoperability specifications that apply.

2.1 Exportable Data

The following categories of data and metadata generated through the EU Customer's use of the Cloud Services are available for export:

Input Data

Files uploaded by Customers to the Cloud Services are not re-exported as part of the switching process, as Customers retain those files and do not require Oktopi to return them.

Output Data

Workflow outputs, reports, and other Service Output generated by the Cloud Services for and on behalf of the Customer, including:

- documents and summaries produced through document review workflows;
- annotated outputs; and
- other output delivered to the Customer through the platform.

Metadata

Metadata associated with the Customer's use of the Cloud Services that is attributable to the Customer, for example audit logs.

Customer-Specific Configurations

Workspace configurations, project settings and other Customer-specific parameters stored within the Cloud Services.

2.2 Digital Assets

The following digital assets created or generated through the Cloud Services, in respect of which the EU Customer holds rights of use independently from its contractual relationship with Oktopi, are available for export. The export package comprises the following files:

- **organisation.json** — Organisation record.

- **workspaces.json** — All workspaces within the Organisation.
- **members.csv** — Full member profiles (includes names, email addresses, and related attributes; GDPR personal data slice).
- **member_preferences.json** — Member preference settings.
- **member_profile.json** — Individual member profile data.
- **access.csv** — Workspace and project access records.
- **projects.json** — All projects within the Organisation.
- **tasks.csv** — Task records.
- **notes.json** — Notes associated with projects and tasks.
- **issues.csv** — Issue records.
- **assessments.json** — Assessment records, including sections, activities and reports (nested).
- **tpp.json** — Target product profile data, including values, transitions and ticks (nested).
- **chat_sessions.json** — AI chat session transcripts, including citations.
- **peer_reviews.json** — Peer review results and feedback.
- **audit.csv** — Audit log records.
- **files_manifest.json** — Metadata manifest for uploaded files (filename, type, size, MIME type, uploader, storage keys, and SHA-256 integrity hash). File content is not re-exported as it comprises the Customer's own uploads.
- **README.txt** — Schema version, export timestamp and integrity hashes for the export package.

2.3 Exempted Data

The following categories of data are expressly excluded from Exportable Data and are not subject to switching or data retrieval obligations. These exclusions exist where disclosure would risk breach of Oktopi's trade secrets, expose cybersecurity vulnerabilities, or involve data that cannot be separated from other customers' data without disproportionate effort:

- Oktopi's proprietary and confidential information, including model weights, training data, algorithm logic, system architecture and trade secrets (such as taxonomies) embedded in or used to generate Service Output;
- data subject to binding legal or regulatory obligations preventing disclosure;
- data that relates exclusively to other customers of Oktopi in a multi-tenancy environment and that cannot be separated from the EU Customer's data without disproportionate effort; and
- anonymised or aggregated data from which the EU Customer cannot be individually identified.

2.4 Data structures and applicable standards

Exportable Data is held in the following structures and formats within the Cloud Services:

- Relational database and AWS Object Store.

The following open standards and interoperability specifications apply to or are available for Exportable Data:

- **Data exchange formats:** JSON & CSV
- **API standards:** REST and GraphQL
- **Character encoding:** UTF-8 (Unicode Standard)

Register 3 — Infrastructure Jurisdictions

This register identifies the jurisdictions to which the ICT infrastructure deployed for data processing in connection with the Cloud Services is or may be subject.

3.1 Primary cloud hosting

Oktopi's Cloud Services are hosted on infrastructure provided by Amazon Web Services (AWS). The following AWS regions are used or may be used in connection with the provision of the Cloud Services:

Primary region	Oktopi hosts Cloud Services across multiple AWS regions: United Kingdom, Germany (Frankfurt), Japan, Australia and the United States. Each region operates as a primary region for the customers it serves, with data stored and processed within the region to support data sovereignty and residency controls.
Secondary / failover region	Oktopi follows AWS best practices for backup, failover and restore processes within each region. Data separation controls prevent cross-region data processing.
Data residency for EU customers	EU customer data is stored and processed exclusively in the Frankfurt, Germany AWS region.

3.2 Sub-processor jurisdictions

In addition to AWS, Oktopi engages sub-processors whose infrastructure may be subject to the laws of the following jurisdictions: Australia (Oktopi Pty Ltd and any Australia-based tooling) and the United States (Amazon Web Services, Inc. and any US-based tooling). AWS entities are engaged in each region in which Oktopi operates, including EU and EEA regions.

Oktopi's current Sub-processor List is available to customers upon reasonable written request addressed to info@oktopi.com.

3.3 Applicable laws

By virtue of the jurisdictions identified above, the ICT infrastructure used in connection with the Cloud Services is or may be subject to the laws of:

- Australia — including the Privacy Act 1988 (Cth) and the Australian Privacy Principles;
- United States — including US federal laws applicable to infrastructure hosted in AWS US regions, including the CLOUD Act and applicable federal and state laws.
- European Union — including the EU GDPR (Regulation (EU) 2016/679), the EU Data Act (Regulation (EU) 2023/2854), and the national implementing laws of Germany, by virtue of EU customer data being hosted in the Frankfurt, Germany AWS region.

Register 4 — Measures to Prevent Unlawful Governmental Access

This register provides a general description of the technical, organisational and contractual measures adopted by Oktopi to prevent international governmental access to or transfer of non-personal data held in the European Union where such access or transfer would conflict with EU law or the law of an EU Member State.

4.1 Contractual measures

Oktopi's agreements with its cloud hosting provider (AWS) and sub-processors include provisions requiring:

- notification to Oktopi of any legally binding governmental request for access to customer data, to the extent permitted by applicable law;
- challenge of requests that are overbroad, unlawful or inconsistent with applicable legal standards; and
- minimisation of data disclosed in response to any governmental request.

Oktopi's own SaaS Framework Agreement includes Standard Contractual Clauses (Module Two: Controller to Processor) which impose obligations on Oktopi to notify EU customers and, where applicable, challenge governmental access requests that conflict with EU law.

4.2 Technical measures

Oktopi implements the following technical measures relevant to preventing unlawful governmental access:

- Encryption at rest: AWS S3 AES-256 with AWS managed keys, RDS and ECS Fargate ephemeral storage
- Encryption in transit: TLS1.2 minimum with TLS1.3 supported
- Access controls: Auth0 controls are used for user identity and access management. User/password access is provisioned as a default, organisations can choose to add MFA or SSO as required. Application RBAC controls enforce least privilege within projects within organisations
- Key management: AWS KMS with customer managed keys with rotation.
- Data residency controls: customer data remains within its designated AWS region and is not transferred to other regions.

4.3 Organisational measures

Oktopi maintains the following organisational measures:

- an information security management system aligned to ISO 27001, currently progressing toward certification;
- an internal data governance framework that classifies customer data and applies appropriate handling controls based on sensitivity;
- staff training on data handling obligations, confidentiality requirements and incident response procedures;
- a designated point of contact (Chief Operating Officer) for all governmental access requests and data protection enquiries; and

- ongoing security monitoring and incident response capability, including infrastructure and application activity monitoring and alerting via AWS CloudWatch and Grafana.

4.4 Reporting

Where Oktopi receives a governmental request for access to customer data (including non-personal data), Oktopi will, to the extent permitted by applicable law:

- notify the affected customer promptly;
- assess the legality of the request and, where there are reasonable grounds, challenge it; and
- provide only the minimum information required in response to any lawful request.

Oktopi will maintain a record of all governmental access requests received and their outcomes, available to competent supervisory authorities on request.