

INFORMATION ON DATA EXPORT OPTIONS AND THE SWITCHING PROCESS (DATA ACT)

(Effective from and last updated on 26 September 2026)

This page provides the information required under Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data (the “**Data Act**”) regarding:

- a) a detailed specification of all categories of data and digital assets transferable during the switching procedure, including at least all exportable data;
- b) a comprehensive specification of categories of data specific to the internal functioning of the service, which are excluded from exportable data under letter (a) of this section,
- c) information on available procedures for switching data processing service providers and data transfer, including available switching methods, transfer formats, and technical and other limitations known to DocReveal;
- d) the data structures and data formats, as well as the relevant standards and open interoperability specifications, in which the exportable data referred to in Article 25(2)(e) of the Data Act are available,
- e) information on the jurisdiction governing the information and communication technology infrastructure used for data processing for the respective services,
- f) a general description of technical, organisational and contractual measures adopted by DocReveal to prevent international access by public authorities to non-personal data stored in the European Union or their transfer, where such access or transfer could conflict with European Union or national law of the relevant Member State.

The rights described on this page apply if and to the extent that the Service is provided as a data processing service within the meaning of the Data Act. To the extent that the provision of the Service does not meet the definition of a data processing service under the Data Act, these rights do not arise for the User.

1. AVAILABLE METHODS FOR SWITCHING TO ANOTHER PROVIDER OF DATA PROCESSING SERVICES AND DATA TRANSFER

The User may switch to another provider of data processing services or migrate to their own on-premises infrastructure. For this purpose, the following methods are available:

- **Self-service data export via the application**

The User may export some of the data (see details below in Section 3) directly from the user interface using the built-in export functions, in particular by downloading the original uploaded documents and files in their original formats and by exporting configuration and audit data in formats which are available in the application for the respective type of data (e.g. JSON, CSV, XML, YAML or XLSX).
- **Assisted export and migration support**

DocReveal provides reasonable assistance with the switching process to the extent set out in Section 10 of the Terms of Service. Any assistance beyond that scope is provided at DocReveal's

discretion and against a reasonable agreed remuneration, as the above-mentioned self-service data export is available to the User for all exportable data.

2. TECHNICAL AND OTHER KNOWN LIMITATIONS

Although DocReveal seeks to make switching and data portability as smooth as possible, the following limitations may apply:

- **Dependencies on third-party services**
If the User uses integrations with third-party tools (e.g. systems connected via integrations available in the application), data in those tools may be subject to their own limitations regarding export, formats or API availability. DocReveal cannot guarantee the portability of data processed exclusively within such third-party environments.
- **Performance and capacity limits**
High-volume or frequent bulk exports may be subject to limitations (rate limits), scheduling or batch processing in order to maintain the stability and performance of the Service for all users.
- **User configuration and the target environment**
Successful import into the target environment (another provider or an on-premises system) depends on the technical capabilities, configuration and data model of that environment. DocReveal does not control and is not responsible for limitations on the side of the target system.

3. CATEGORIES OF EXPORTABLE DATA AND DIGITAL ASSETS, DATA STRUCTURES AND FORMATS

3.1 Categories of exportable data and digital assets

- **Documents and files**
 - Original documents and files uploaded by the User (in the original file format), either on a file-by-file basis or as a whole folder within the folder structure of the application's interface
- **Configuration and audit data**
 - All configuration and audit data available in the application, in the respective section and for the respective functional area or its part. For example activity data such as the audit trail, the list of users, the purchased Subscription plans or the records of configuration changes
 - Exports are available in the formats offered by the application for the respective data set (usually JSON, CSV, XML, YAML or XLSX) and must be done separately for each functional area or its part
- **Agents, integration flows and data models**
 - The configuration of AI agents (exported without secrets and connections), integration flows (workflows) and their runs, and data model schemas, each exported in JSON through the export function of the respective section.

- **Conversation outputs**

- Individual answers generated in conversations with the AI features, which can be copied or downloaded in Markdown or DOCX format.

Notwithstanding the above, data for which the application does not offer an export function are not exportable (see Sections 3.2 and 3.3).

3.2 Categories of data that cannot be exported

- **Extracted and derived data (internal memory of the Service)**

Data which the Service derives from the User's uploaded content and which form the internal "memory" of the User's workspace – in particular vector embeddings, entities and relationships stored in the graph database, analytics records and other internal representations of the uploaded documents and data. These are stored in a proprietary format and structure specific to the internal functioning of the Service, which cannot be read or used outside the Service. The User does not have, and is not intended to have, direct access to them within the Service either. They serve solely as the basis on which the AI features of the Service answer the User's questions and generate outputs in conversations. As these data embody the User's know-how in a form that can only be interpreted by the Service, they are not exportable and are not transferred to third parties; the underlying original documents may be exported under Section 3.1 and re-processed in the target environment.

- **Internal artefacts**

Internal artefacts that the Service creates on the basis of the User's data for its own functioning (e.g. adaptations of extraction behaviour based on the User's corrections) embody know-how processed by the Service; their export is not enabled in the Service and they are therefore not exportable. The configuration of AI agents, integration flows and data model schemas is exportable under Section 3.1 (without secrets, credentials and connections – see below).

- **Conversation history (chats)**

Conversations with the AI features of the Service are stored in the User's workspace for the retention period set in the application (by default 365 days from the last activity), and the User may delete them at any time. Individual answers can be copied or downloaded during the conversation (see Section 3.1); an export of the entire conversation history is not offered.

- **Configuration of payment and security integrations**

Specific parameters posing a security risk and directly tied to the system integration at the technical level (e.g. the configuration of the Stripe payment integration, API keys and security credentials, and internal security and operational logs).

3.3 Categories of data for which switching is very complex, costly, or for which switching is not possible without significant changes to the architecture of data, digital assets or services

- **Cloud database services**

For the smoothest possible operation of the Service, DocReveal uses a proprietary data model and table structure developed by DocReveal, as well as specific database functions and procedures,

including an internal data format, which in this configuration exist only with DocReveal. A transfer may therefore require, in particular, a redesign of the database schema and conversion of data into another format.

4. ICT INFRASTRUCTURE AND RELEVANT JURISDICTIONS

- Data are stored in the AWS cloud in the EU (Amazon Web Services, region EU North – Stockholm, Sweden (eu-north-1)), including infrastructure-level backups of the cloud provider for DocReveal's operational purposes, which are not available to Users and are automatically erased no later than thirty-five (35) days after the deletion of the data. DocReveal may also use other AWS regions located in the European Union (e.g. Ireland) for redundancy or cost optimization; data always remain within the European Union.
- the relevant jurisdiction in relation to the primary cloud infrastructure is the Kingdom of Sweden; where other EU regions are used, the relevant jurisdiction is the respective EU Member State (e.g. Ireland).

5. MEASURES AGAINST UNAUTHORISED INTERNATIONAL ACCESS BY PUBLIC AUTHORITIES

DocReveal is committed to ensuring that any international access by public authorities to non-personal data stored in the EU takes place in accordance with applicable EU and Member State law. DocReveal has implemented a combination of technical, organisational and contractual measures designed to prevent access or to challenge access requests that would conflict with EU law or national law.

Technical measures include, inter alia:

- **Logical and physical separation of environments**

Data stored in the EU are hosted in data centers in the EU and are logically and physically separated from other environments.

- **Access control and the principle of least privilege**

Access to production systems is strictly controlled, logged and restricted to authorised persons based on their role and need-to-know.

- **Encryption**

Data are protected in transit and at rest using industry-standard encryption mechanisms, to the extent enabled by the relevant infrastructure and services used.

These measures reduce the risk that foreign public authorities obtain direct access to data via infrastructure providers without using appropriate legal channels.

Organisational and contractual measures include:

- **Contractual commitments of providers**

DocReveal requires from its cloud and infrastructure providers to comply with applicable EU law and—where permitted by law—to inform DocReveal of any legally binding requests by public authorities for

access to data. Standard Contractual Clauses (SCCs) are also agreed between DocReveal and the infrastructure provider where relevant.

• Internal procedures for handling requests

If DocReveal receives a request from a public authority outside the EU/EEA for access to data stored in the EU, DocReveal will:

- carefully assess the legal basis for such request,
- verify whether the request is compatible with EU law and the relevant national law, and
- challenge or oppose the request if DocReveal reasonably believes it conflicts with such laws or exceeds the requesting authority's powers.

• Transparency towards users

Unless legally prohibited, DocReveal will inform the affected Users without undue delay of such a request and the data concerned so that they can take appropriate steps to protect their interests.