Data Location and Data Export

Information under the Data Act (Regulation (EU) 2023/2854). Last updated: November 2026

This English version is provided for convenience. In the event of any discrepancy, the German version prevails.

Infrastructure and Governing Law

We store and process our customers' content and exportable data exclusively in data centers of Scaleway SAS in the Paris metropolitan area, without any transfer to third countries. This also applies to storage in Asset Management and to our AI models. The infrastructure used is subject to French law and the law of the European Union; the contracting party is on:mint GmbH, based in Berlin. The public Polygon blockchain holds only hash values, from which content cannot be reconstructed.

Protection Against Access from Third Countries

We take the following measures against unlawful access by governmental authorities outside the EU to data that we store in the EU:

- Technical: encryption of every transmission with Transport Layer Security (TLS) 1.2 or 1.3 and encrypted storage of stored files; keys in Scaleway's Key Manager in the EU; storage nodes and core services in private networks without public access.
- Organizational: access only by authorized employees under a role-based access concept; legal review of every disclosure request from an authority before we respond to it.
- Contractual: only sub-processors with processing locations in the EU, without transfers to third countries. We disclose data to authorities of a third country only on the basis of an international agreement or within the limits of Article 32 of the Data Act. Before doing so, we inform the affected customer to the extent permitted.

Exportable Data, Formats, and Interfaces

Which data is exportable and which is not is conclusively governed by Section 9(1) of our Terms. Customers can retrieve their data during the term of the contract and for 30 calendar days after the contract ends. For export and switching, we provide all customers with a documented export interface free of charge; in plans without access to the application programming interface (API), upon request.

Data	Format	Retrieval
Uploaded and stored files	Original format, such as JPEG, PNG, WebP, PDF, MP4	Account, export interface
Labeled files with label, watermark, and Content Credentials	Image or video format with an embedded manifest based on the standard of the Coalition for Content Provenance and Authenticity (C2PA); for PDF documents, the manifest as a separate file	Account, export interface
Content Credentials manifests	C2PA manifest according to the C2PA specification in JPEG Universal Metadata Box Format (JUMBF), additionally as JSON (JavaScript Object Notation)	Export interface
Logs and registers: labels, exceptions, work history in IP Management	JSON and CSV (comma-separated values)	Account, export interface

Data	Format	Retrieval
Anchors	Hash value, timestamp, and transaction ID as JSON	Export interface; also publicly verifiable on the blockchain
Account and labeling settings	JSON	Export interface

Known Limitations

Content Credentials remain linked to on:mint's signing certificate. A new provider can read and verify existing manifests but cannot continue them in on:mint's name. Invisible watermarks can be read only with on:mint's methods; verification remains available free of charge through on:mint Verify for as long as on:mint Verify is offered.

Switching Providers

The process and deadlines for switching are governed by Section 9 of our Terms. You announce a switch or the erasure of your data in text form, for example by email to hello@onmint.io. We do not impose switching charges.