Data Processing Agreement (DPA) for the Services of on:mint GmbH

Annex to the General Terms and Conditions of on:mint GmbH. Last updated: November 2026

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

1. Subject Matter, Duration, and Scope

1.1 on:mint GmbH ("Provider") processes personal data exclusively on behalf of the customer ("Customer") within the scope of the services owed under the contract for the use of the Services ("Processing"). This contract comprises the General Terms and Conditions of on:mint GmbH (Terms), the selected plan, and any offers ("Main Agreement"). Terms defined in the Main Agreement have the same meaning here.

1.2 The subject matter of the Processing is the handling and, to the extent booked, the storage of the Customer's content in the Services, in particular Content Credentials, AI labeling with mintys, IP Management, and Asset Management. The Processing comprises receiving files via the app, the application programming interface (API), or the MCP server; AI detection and preliminary assessment; embedding labels, watermarks, and Content Credentials; signing; generating and anchoring hash values; storage; provision for download; public provenance records at the Customer's option; logging of labeling and work steps; and deletion. The purpose is the provision of the Services under the Main Agreement. This DPA applies for as long as the Provider processes personal data for the Customer.

1.3 The Processing concerns in particular the following categories of data subjects and data: (a) persons depicted or named in content: image, video, and audio recordings, documents, names, and other information in content and metadata, such as information in the Exchangeable Image File Format (EXIF), including the location where a recording was made; (b) authors, editors, and rights holders: names, identifiers, and information on creation, tools, and editing steps as recorded in Content Credentials or in IP Management; (c) the Customer's users: names, user IDs, email addresses, and timestamps in logs, such as who labeled what and when. The nature and scope of the content are determined solely by the Customer. Content may contain special categories of personal data within the meaning of Article 9 GDPR; the Provider does not process such data in a targeted manner. AI detection does not serve to identify natural persons; the Provider does not process biometric data for the purpose of uniquely identifying a natural person.

1.4 The Customer remains the controller within the meaning of Article 4(7) GDPR. The Provider processes the data as a processor under Article 28 GDPR. If the Customer in turn processes the data on behalf of a third party, for example as an agency for its clients, the Provider is another processor (sub-processor) within the meaning of Article 28(4) GDPR; the Customer ensures that the controller's required authorization is in place.

1.5 This DPA does not cover the processing of personal data that the Provider carries out as a controller for its own purposes. This includes in particular the management of the contractual relationship, including billing and payment processing through payment service providers, the management of user accounts and logins, the security of the Services, the analysis of usage data under Section 6(2) of the Terms, and the use of on:mint Verify without an account.

1.6 If the Customer initiates the transfer of content to third-party services, such as publication on social networks or the connection of its own systems and AI tools via the API or the MCP server, this constitutes an instruction. These services are not sub-processors of the Provider; the Customer is responsible for their use. The same applies to information that the Customer releases as a public provenance record.

2. Instructions

2.1 The Provider processes personal data only on documented instructions from the Customer, including with regard to transfers to a third country or an international organization, unless required to do so by Union or Member State law to which the Provider is subject. In such a case, the Provider informs the Customer before processing, to the extent that such information is legally permissible.

2.2 The Main Agreement, including this DPA, constitutes the initial instructions. The Customer also issues instructions through settings and requests in the Services, for example regarding the labeling standard, storage, the release of public provenance records, and deletion, as well as via the API or the MCP server. Further instructions may be given in text form. The Customer confirms oral instructions in text form without undue delay.

2.3 If the Provider considers an instruction to be unlawful, it informs the Customer without undue delay. The Provider is entitled to suspend the execution of the instruction until it is confirmed or changed, to the extent necessary to avoid a violation of the law.

2.4 The Provider may provide services beyond the contractually agreed Processing, in particular additional instructions, support, or documentation, in return for reasonable remuneration, unless the Main Agreement provides otherwise. This does not apply to the extent that the effort was caused by a breach of this DPA or of the GDPR for which the Provider is responsible.

3. Confidentiality

3.1 The Provider ensures that the persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1 The Provider implements the technical and organizational measures required under Article 32 GDPR. In doing so, it takes into account in particular the state of the art, the costs of implementation, the nature, scope, context, and purposes of the processing, and the likelihood and severity of the risks to the rights and freedoms of natural persons. The measures in place when the contract is concluded are described in Annex 2.

4.2 The Provider reviews its technical and organizational measures and adapts them as needed. The Customer has no entitlement to the retention of specific measures, provided that the level of protection required by Article 32 GDPR is maintained.

5. Assistance to the Customer

5.1 Taking into account the nature of the processing and the information available to it, the Provider assists the Customer by appropriate technical and organizational measures in responding to requests from data subjects under Articles 12 to 22 GDPR.

5.2 If a data subject asserts claims directly against the Provider, the Provider forwards the request to the Customer without undue delay. The Provider does not respond to the request itself unless it is legally obligated to do so or has been instructed to do so by the Customer.

5.3 Taking into account the nature of the processing and the information available to it, the Provider assists the Customer in complying with its obligations under Articles 32 to 36 GDPR, in particular regarding the security of processing, the notification of personal data breaches, data protection impact assessments, and prior consultations.

5.4 If the Provider becomes aware of a personal data breach affecting data processed on behalf of the Customer, it informs the Customer without undue delay after becoming aware of it, and in any event within 48 hours, and provides the available information to the extent necessary for the Customer to

comply with its obligations under Articles 33 and 34 GDPR.

6. Sub-processors

6.1 The Customer grants the Provider general written authorization to engage sub-processors.

6.2 The Provider informs the Customer in text form before engaging a new sub-processor or replacing an existing one and keeps the current list available on its website. The Customer may object for a valid reason within 14 calendar days after receiving the information. If no timely objection is made, the change is deemed approved.

6.3 In the event of a justified objection, the Provider will not use the sub-processor for the Customer, and the parties will seek an appropriate solution. If no such solution is possible, or if the Provider cannot reasonably be expected to provide the services without the sub-processor, either party may terminate the affected plans for cause; the Provider refunds fees paid in advance on a pro rata basis.

6.4 The Provider contractually imposes on each sub-processor essentially the same data protection obligations as those set out in this DPA, in particular appropriate technical and organizational measures under Article 32 GDPR. The Provider remains responsible to the Customer for the performance of the sub-processor's obligations (Article 28(4) GDPR).

6.5 The sub-processors engaged when the contract is concluded are listed in Annex 1.

7. Processing in Third Countries

7.1 Personal data is transferred or processed outside the European Union or the European Economic Area (third country) only on documented instructions from the Customer and only if the specific requirements of Articles 44 et seq. GDPR are met.

7.2 The approval of a sub-processor with a processing location in a third country constitutes an instruction to carry out this transfer.

7.3 To the extent that the Provider or a sub-processor processes data in a third country, the Provider ensures an appropriate legal basis for the transfer.

7.4 To prove the existence, time, and integrity of a file, the Provider stores on a public blockchain, currently Polygon, exclusively hash values (digital fingerprints) and technical identifiers, no content. A file cannot be reconstructed from a hash value; only someone who possesses the file itself can match it. The Provider stores mapping data exclusively in the EU. The operators of the blockchain nodes have no access to content and are not sub-processors. Anchors cannot be technically deleted (Section 4(4) of the Terms).

8. Proof of Compliance and Audits

8.1 Upon request, the Provider makes available to the Customer the information necessary to demonstrate compliance with the obligations under Article 28 GDPR. For this purpose, the Provider may in particular present current certificates, reports from independent bodies, or self-assessments.

8.2 The Provider allows for and contributes to audits, including inspections, conducted by the Customer or by an auditor mandated by the Customer. A mandated auditor must be bound by confidentiality and must not be in a direct competitive relationship with the Provider.

8.3 Audits generally take place during normal business hours, with due regard for the Provider's operations and with reasonable advance notice, unless an audit without notice appears necessary because the purpose of the audit would otherwise be jeopardized.

8.4 The Customer treats as confidential any information about the Provider obtained in the course of proof of compliance and audits. However, the Customer may disclose such information to supervisory authorities and data subjects to the extent necessary to demonstrate the lawfulness of the processing.

8.5 Each party bears its own costs arising from an audit. For the second and each further inspection within a calendar year, the Provider may charge reasonable remuneration unless the inspection is carried out at the request of a supervisory authority. If the audit was prompted by a breach of this DPA or of the GDPR for which the Provider is responsible, the Provider bears the costs.

9. Return and Deletion

9.1 When the Main Agreement or a booked storage plan ends, the Customer may export its data during the retrieval period under Section 9(4) of the Terms (return). Thereafter, the Provider deletes the personal data concerned unless Union or Member State law requires its storage; the Provider restricts the processing of such data for other purposes and deletes it upon expiry of the retention period. On the Customer's instructions, register entries and provenance records remain in place beyond the end of the contract.

9.2 Without booked storage, the Provider keeps files only for as long as necessary for processing and download. If the Customer deletes files in the Services, the Provider deletes them, including any associated public provenance records; anchors under clause 7.4 remain in place.

9.3 Deletion takes place without undue delay, and in any event within 30 days, as part of the Provider's regular technical deletion procedures. Data in backup copies is deleted no later than when the backups are overwritten in the regular cycle, to the extent that earlier deletion is technically impossible or possible only with disproportionate effort. Until deletion, the data is not processed in productive operation unless required by law. To that extent, this DPA continues to apply until complete deletion.

10. Miscellaneous

10.1 Liability is governed by the Main Agreement (Section 10 of the Terms); Article 82 GDPR remains unaffected.

10.2 Further statutory obligations of the Provider remain unaffected.

10.3 In the event of any conflict between this DPA and the Main Agreement, this DPA prevails to the extent that the processing of personal data on behalf of the Customer is concerned.

10.4 Section 12(2) of the Terms applies accordingly to amendments of this DPA.

Annex 1: Approved Sub-processors

Sub-processor	Service	Processing location	Safeguards
Scaleway SAS, 8 rue de la Ville-l'Évêque, 75008 Paris, France (Paris Trade and Companies Register 433 115 904)	Hosting of the platform, of the AI models for AI detection and preliminary assessment, and of content-based storage in Asset Management: managed Kubernetes, load balancer, private network, messaging, Key Manager, Secret Manager, object storage	France, data centers in the Paris metropolitan area	Processing exclusively in the EU, no transfer to third countries; further data center operators per www.scaleway.com/en/subprocessorlist

Annex 2: Technical and Organizational Measures

Last updated: November 2026. The Provider operates the platform, its AI models, and the storage nodes exclusively in Scaleway data centers in the Paris metropolitan area (Annex 1), without any transfer to third countries. Scaleway ensures the physical security of the data centers through an information security management system certified under ISO/IEC 27001:2022.

Organization (Article 32(1)(b) and (d) GDPR)

Responsibilities: Definition of binding responsibilities for information security and data protection; security policy approved by management; documented escalation and reporting channels for security incidents.

Personnel: Commitment of all employees to confidentiality; training on data protection and information security upon joining and at least annually, including defense against phishing and social engineering; structured onboarding and offboarding process with granting and revocation of access rights.

Encryption and Pseudonymization (Article 32(1)(a) GDPR)

Data at rest: Encrypted storage of stored files on the storage nodes; access only via the respective Customer's access token; storage of keys separately from the data.

Key management: Management of credentials in Scaleway's Secret Manager and of signing keys in Scaleway's Key Manager; credentials passed to the services only at startup and only via TLS; signing operations, including for Content Credentials, exclusively via the Key Manager.

External connections: TLS 1.3, with TLS 1.2 as the minimum version; TLS 1.0 and 1.1 are rejected; for TLS 1.2, exclusively ECDHE key exchange with AEAD ciphers (AES-GCM, ChaCha20-Poly1305), thus providing perfect forward secrecy; TLS termination only at the ingress within the cluster, with the load balancer passing encrypted traffic through unchanged; certificates from Let's Encrypt with automatic renewal; HSTS for web access.

Internal connections: Communication between services predominantly asynchronous via Scaleway's messaging service, with separate credentials for each service and via TLS; encryption of traffic between cluster nodes with WireGuard; connections to Key Manager, Secret Manager, and object storage exclusively via TLS; no unencrypted protocols.

Cryptography: Use of recognized state-of-the-art algorithms, such as AES-256 and SHA-256 or stronger; no algorithms with known weaknesses such as MD5, SHA-1, or DES; regular review of the algorithms used.

Blockchain:	Storage exclusively of hash values and technical identifiers, no content (clause 7.4).
Pseudonymization:	Internal referencing of files via random or content-based identifiers.

Confidentiality (Article 32(1)(b) GDPR)

Physical access control:	No in-house server rooms; operation exclusively in Scaleway's certified data centers.
System access control:	Access to administrative functions only with multi-factor authentication and key pairs, without password login; operation of the cluster in a private network (Scaleway VPC) without a shared network segment with other customers; core services and storage nodes without public access; default-deny network policies in the cluster; server hardening and deactivation of unneeded services.
User accounts:	Personal identifiers, no group accounts; passwordless login via social login or a one-time code by email, each with multi-factor authentication; no storage of passwords by the Provider.
Data access control:	Role and authorization concept based on the need-to-know principle; separate administrator and user identifiers; no work with root accounts in regular operation; review of authorizations at least annually; employee access to the Customer's content only to the extent necessary for support or troubleshooting, and documented.
Separation control:	Separation of tenants per Customer; separate production, test, and development environments; no processing of the Customer's content in test or development environments and no training of AI models with this content.
Endpoints:	Disk encryption, automatic screen lock, malware protection, and automatic security updates on all business devices; no storage of the Customer's content on endpoints; loss reporting and remote wipe of mobile devices.

Integrity (Article 32(1)(b) GDPR)

Transfer control:	Operation of the storage nodes as a private network with a 256-bit network key, without connection to public storage networks and without a public gateway; retrieval of files only when authenticated and encrypted; public provenance records only with the information released by the Customer.
API and MCP server:	Access only with personal API keys; rate limiting per key; revocation of keys in the account.
Input control:	Traceability of who uploaded, labeled, or deleted which file and when; proof of integrity through hash values, signing of Content Credentials, and anchoring on the blockchain.
Content-based storage:	Referencing of each file in Asset Management by its hash value rather than by folders and file names, so that any modification is detectable.
Logging:	Recording of administrative logins and access to the infrastructure in Scaleway's audit trail; use of logs only for security and verification purposes.

Availability, Resilience, and Recoverability (Article 32(1)(b) and (c) GDPR)

Redundancy:	Storage of each stored file on multiple storage nodes in separate availability zones.

Backup:	Backups according to a documented concept; encrypted backup copies at a physically separate location; at least one backup that is immutable or separated from the production system (protection against ransomware); regular restore tests.
Business continuity:	Emergency and recovery plan, including ransomware and infrastructure provider failure scenarios; regular exercises; documented exit strategy for switching providers.
Operations:	System monitoring with alerting; patch management with prompt installation of critical security updates; DDoS protection by Scaleway.

Procedures for Regular Review (Article 32(1)(d) GDPR)

Review:	Review and adjustment of these measures at least annually and in the event of significant changes; regular vulnerability assessments and penetration tests.
Development:	Data protection by design and by default (Article 25 GDPR); code reviews; automated scanning of code and dependencies for vulnerabilities; inventory of the components used; no credentials in the Provider's source code management; security testing according to recognized methods, such as those of the Open Worldwide Application Security Project (OWASP).
Security incidents:	Procedure for detecting, assessing, and reporting security incidents, including notification of the Customer under clause 5.4; documentation of every incident.
Processor control:	Engagement of sub-processors only in accordance with Annex 1, on the basis of a contract under Article 28 GDPR and documented safeguards, in particular ISO/IEC 27001; annual review based on current certificates; monitoring of changes to Scaleway's sub-processors; no administrative access for external service providers to the Provider's systems; documentation of instructions.
Deletion:	Unpinning and garbage collection on all storage nodes as well as deletion of the associated keys and mapping data; deactivation of associated access tokens and public provenance records; backup copies in accordance with clause 9.3; confirmation of deletion in text form upon request.