Auftragsverarbeitungsvertrag (AVV) für die Dienste der on:mint GmbH

Anlage zu den Allgemeinen Geschäftsbedingungen der on:mint GmbH. Stand: November 2026

1. Gegenstand, Dauer und Umfang

1.1 Die on:mint GmbH („Auftragnehmer“) verarbeitet personenbezogene Daten ausschließlich im Auftrag des Kunden („Auftraggeber“) im Rahmen der Leistungen, die nach dem Vertrag über die Nutzung der Dienste geschuldet sind („Verarbeitung“). Dieser Vertrag umfasst die Allgemeinen Geschäftsbedingungen der on:mint GmbH (AGB), das gewählte Paket und etwaige Angebote („Hauptvertrag“). Begriffe des Hauptvertrags haben hier dieselbe Bedeutung.

1.2 Gegenstand der Verarbeitung ist die Bearbeitung und, soweit gebucht, die Speicherung der Inhalte des Auftraggebers in den Diensten, insbesondere Content Credentials, KI-Kennzeichnung mit mintys, IP Management und Asset Management. Die Verarbeitung umfasst die Entgegennahme von Dateien über App, Programmierschnittstelle (API) oder MCP-Server, die KI-Erkennung und Vorprüfung, das Einbetten von Label, Wasserzeichen und Content Credentials, die Signatur, die Hashwertbildung und Verankerung, die Speicherung, die Bereitstellung zum Download, öffentliche Nachweise auf Wahl des Auftraggebers, die Protokollierung von Kennzeichnungs- und Arbeitsschritten sowie die Löschung. Zweck ist die Erbringung der Dienste nach dem Hauptvertrag. Dieser AVV gilt, solange der Auftragnehmer personenbezogene Daten für den Auftraggeber verarbeitet.

1.3 Die Verarbeitung betrifft insbesondere folgende Personengruppen und Daten: (a) in Inhalten abgebildete oder genannte Personen: Bild-, Video- und Tonaufnahmen, Dokumente, Namen und sonstige Angaben in Inhalten und Metadaten, etwa Angaben im Exchangeable Image File Format (EXIF) einschließlich des Aufnahmeorts; (b) Urheber, Bearbeiter und Rechteinhaber: Namen, Kennungen und Angaben zu Erstellung, Werkzeugen und Bearbeitungsschritten, wie sie in Content Credentials oder im IP Management festgehalten werden; (c) Nutzer des Auftraggebers: Namen, Benutzerkennungen, E-Mail-Adressen und Zeitstempel in Protokollen, etwa wer wann gekennzeichnet hat. Art und Umfang der Inhalte bestimmt allein der Auftraggeber. Inhalte können besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO enthalten; der Auftragnehmer verarbeitet sie nicht gezielt. Die KI-Erkennung dient nicht der Identifizierung natürlicher Personen; biometrische Daten zur eindeutigen Identifizierung verarbeitet der Auftragnehmer nicht.

1.4 Der Auftraggeber bleibt Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Der Auftragnehmer verarbeitet die Daten als Auftragsverarbeiter gemäß Art. 28 DSGVO. Verarbeitet der Auftraggeber die Daten seinerseits im Auftrag eines Dritten, etwa als Agentur für deren Kunden, ist der Auftragnehmer weiterer Auftragsverarbeiter im Sinne von Art. 28 Abs. 4 DSGVO; der Auftraggeber stellt die erforderliche Genehmigung des Verantwortlichen sicher.

1.5 Nicht Gegenstand dieses AVV ist die Verarbeitung personenbezogener Daten, die der Auftragnehmer als Verantwortlicher zu eigenen Zwecken vornimmt. Dazu gehören insbesondere die Verwaltung der Vertragsbeziehung einschließlich Abrechnung und Zahlungsabwicklung über Zahlungsdienstleister, die Verwaltung der Nutzerkonten und der Anmeldung, die Sicherheit der Dienste, die Auswertung von Nutzungsdaten nach § 6 Abs. 2 AGB und die Nutzung von on:mint Verify ohne Konto.

1.6 Veranlasst der Auftraggeber die Übermittlung von Inhalten an Dienste Dritter, etwa die Veröffentlichung in sozialen Netzwerken oder die Anbindung eigener Systeme und KI-Werkzeuge über API oder MCP-Server, gilt dies als Weisung. Diese Dienste sind keine Unterauftragsverarbeiter des Auftragnehmers; ihren Einsatz verantwortet der Auftraggeber. Dasselbe gilt für Angaben, die der Auftraggeber als öffentlichen Nachweis freigibt.

2. Weisungen

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, auch in Bezug auf die Übermittlung an ein Drittland oder eine internationale Organisation, sofern keine Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaats besteht, dem der Auftragnehmer unterliegt. In diesem Fall informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung, soweit diese Information rechtlich zulässig ist.

2.2 Der Hauptvertrag einschließlich dieses AVV gilt als anfängliche Weisung. Weisungen erteilt der Auftraggeber außerdem durch Einstellungen und Aufrufe in den Diensten, etwa zu Kennzeichnungsstandard, Speicherung, Freigabe öffentlicher Nachweise und Löschung sowie über API oder MCP-Server. Weitere Weisungen können in Textform erfolgen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

2.3 Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Auftraggeber unverzüglich. Er ist berechtigt, die Ausführung der Weisung bis zu deren Bestätigung oder Änderung auszusetzen, soweit dies zur Vermeidung eines Rechtsverstoßes erforderlich ist.

2.4 Leistungen, die über die vertraglich vereinbarte Verarbeitung hinausgehen, insbesondere zusätzliche Weisungen, Unterstützung oder Dokumentation, kann der Auftragnehmer gegen angemessene Vergütung erbringen, soweit der Hauptvertrag nichts anderes bestimmt. Dies gilt nicht, soweit der Aufwand durch einen vom Auftragnehmer zu vertretenden Verstoß gegen diesen AVV oder die DSGVO verursacht wurde.

3. Vertraulichkeit

3.1 Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4. Sicherheit

4.1 Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Er berücksichtigt dabei insbesondere den Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen. Die bei Vertragsschluss getroffenen Maßnahmen beschreibt Anhang 2.

4.2 Der Auftragnehmer überprüft seine technischen und organisatorischen Maßnahmen und passt sie bei Bedarf an. Ein Anspruch des Auftraggebers auf Beibehaltung bestimmter Maßnahmen besteht nicht, sofern das durch Art. 32 DSGVO geforderte Schutzniveau nicht unterschritten wird.

5. Unterstützung des Auftraggebers

5.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen betroffener Personen nach Art. 12 bis 22 DSGVO.

5.2 Macht eine betroffene Person Ansprüche unmittelbar gegenüber dem Auftragnehmer geltend, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter. Der Auftragnehmer beantwortet das Ersuchen nicht selbst, es sei denn, er ist hierzu rechtlich verpflichtet oder vom Auftraggeber angewiesen.

5.3 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei dessen Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

5.4 Stellt der Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten fest, die im Auftrag verarbeitete Daten betrifft, informiert er den Auftraggeber unverzüglich nach Kenntniserlangung, spätestens binnen 48 Stunden, und stellt die verfügbaren Informationen zur Verfügung, soweit dies für die Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DSGVO erforderlich ist.

6. Unterauftragsverarbeiter

6.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine schriftliche Genehmigung, Unterauftragsverarbeiter einzusetzen.

6.2 Der Auftragnehmer informiert den Auftraggeber vor dem Einsatz eines neuen oder dem Wechsel eines bestehenden Unterauftragsverarbeiters in Textform und hält die aktuelle Liste auf seiner Website bereit. Der Auftraggeber kann aus sachlichem Grund innerhalb von 14 Kalendertagen nach Zugang der Information widersprechen. Erfolgt kein fristgerechter Widerspruch, gilt die Änderung als genehmigt.

6.3 Im Fall eines berechtigten Widerspruchs setzt der Auftragnehmer den Unterauftragsverarbeiter nicht für den Auftraggeber ein, und die Parteien streben eine sachgerechte Lösung an. Ist diese nicht möglich oder dem Auftragnehmer die Leistungserbringung ohne den Unterauftragsverarbeiter nicht zumutbar, kann jede Partei die betroffenen Pakete außerordentlich kündigen; im Voraus gezahlte Entgelte erstattet der Auftragnehmer anteilig.

6.4 Der Auftragnehmer verpflichtet den Unterauftragsverarbeiter vertraglich im Wesentlichen auf dieselben Datenschutzpflichten, die in diesem AVV festgelegt sind, insbesondere auf geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich (Art. 28 Abs. 4 DSGVO).

6.5 Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter ergeben sich aus Anhang 1.

7. Verarbeitung in Drittländern

7.1 Eine Übermittlung oder Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Drittland) erfolgt nur auf dokumentierte Weisung des Auftraggebers und nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

7.2 Die Genehmigung eines Unterauftragsverarbeiters mit Verarbeitungsort im Drittland gilt als Weisung zu dieser Übermittlung.

7.3 Soweit der Auftragnehmer oder ein Unterauftragsverarbeiter Daten in einem Drittland verarbeitet, stellt der Auftragnehmer eine geeignete Rechtsgrundlage für die Übermittlung sicher.

7.4 Zum Nachweis von Existenz, Zeitpunkt und Unversehrtheit einer Datei speichert der Auftragnehmer auf einer öffentlichen Blockchain, derzeit Polygon, ausschließlich Hashwerte (digitale Fingerabdrücke) und technische Kennungen, keine Inhalte. Aus einem Hashwert lässt sich die Datei nicht rekonstruieren; zuordnen kann ihn nur, wer die Datei selbst besitzt. Zuordnungsdaten speichert der Auftragnehmer ausschließlich in der EU. Die Betreiber der Blockchain-Knoten erhalten keinen Zugriff auf Inhalte und sind keine Unterauftragsverarbeiter. Verankerungen sind technisch nicht löschbar (§ 4 Abs. 4 AGB).

8. Nachweise und Prüfungen

8.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage die erforderlichen Informationen zum Nachweis der Pflichten nach Art. 28 DSGVO zur Verfügung. Er kann hierfür insbesondere aktuelle Zertifikate, Prüfberichte unabhängiger Stellen oder Selbstauskünfte vorlegen.

8.2 Der Auftragnehmer ermöglicht Überprüfungen einschließlich Inspektionen, die vom Auftraggeber oder einem von diesem beauftragten Prüfer durchgeführt werden, und trägt dazu bei. Ein beauftragter Prüfer muss zur Vertraulichkeit verpflichtet sein und darf nicht in einem unmittelbaren Wettbewerbsverhältnis zum Auftragnehmer stehen.

8.3 Überprüfungen finden in der Regel während der üblichen Geschäftszeiten, unter angemessener Berücksichtigung der Betriebsabläufe des Auftragnehmers und mit angemessener Vorankündigung statt, sofern nicht eine Überprüfung ohne Ankündigung erforderlich erscheint, weil andernfalls der Kontrollzweck gefährdet wäre.

8.4 Informationen über den Auftragnehmer, die der Auftraggeber im Rahmen von Nachweisen und Überprüfungen erlangt, behandelt er vertraulich. Er darf sie jedoch Aufsichtsbehörden und betroffenen Personen offenlegen, soweit dies zum Nachweis der Rechtmäßigkeit der Verarbeitung erforderlich ist.

8.5 Jede Partei trägt die ihr durch eine Prüfung entstehenden Kosten selbst. Für die zweite und jede weitere Inspektion innerhalb eines Kalenderjahres kann der Auftragnehmer eine angemessene Vergütung verlangen, es sei denn, die Inspektion erfolgt auf Verlangen einer Aufsichtsbehörde. Ist die Prüfung durch einen vom Auftragnehmer zu vertretenden Verstoß gegen diesen AVV oder die DSGVO veranlasst, trägt der Auftragnehmer die Kosten.

9. Rückgabe und Löschung

9.1 Endet der Hauptvertrag oder eine gebuchte Speicherung, kann der Auftraggeber seine Daten während des Abrufzeitraums nach § 9 Abs. 4 AGB exportieren (Rückgabe). Danach löscht der Auftragnehmer die betroffenen personenbezogenen Daten, sofern nicht nach dem Recht der Europäischen Union oder eines Mitgliedstaats eine Pflicht zur Speicherung besteht; solche Daten sperrt er für andere Zwecke und löscht sie nach Ablauf der Aufbewahrungsfrist. Auf Weisung des Auftraggebers bleiben Registereinträge und Nachweise über das Vertragsende hinaus bestehen.

9.2 Ohne gebuchte Speicherung hält der Auftragnehmer Dateien nur so lange vor, wie es für Verarbeitung und Download erforderlich ist. Löscht der Auftraggeber Dateien in den Diensten, löscht der Auftragnehmer sie einschließlich zugehöriger öffentlicher Nachweise; Verankerungen nach Ziffer 7.4 bleiben bestehen.

9.3 Die Löschung erfolgt unverzüglich, spätestens binnen 30 Tagen, im Rahmen der regulären technischen Löschkonzepte des Auftragnehmers. Daten in Sicherungskopien werden spätestens mit deren turnusmäßiger Überschreibung gelöscht, soweit eine frühere Löschung technisch nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Bis zur Löschung werden die Daten nicht produktiv verarbeitet, sofern dies nicht gesetzlich erforderlich ist. Insoweit gilt dieser AVV bis zur vollständigen Löschung fort.

10. Sonstige Bestimmungen

10.1 Für die Haftung gilt der Hauptvertrag (§ 10 AGB); Art. 82 DSGVO bleibt unberührt.

10.2 Weitergehende gesetzliche Pflichten des Auftragnehmers bleiben unberührt.

10.3 Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag geht dieser AVV vor, soweit es um die Verarbeitung personenbezogener Daten im Auftrag geht.

10.4 Für Änderungen dieses AVV gilt § 12 Abs. 2 AGB entsprechend.

Anhang 1: Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Verarbeitungsort	Garantien
Scaleway SAS, 8 rue de la Ville-l'Évêque, 75008 Paris, Frankreich (Handelsregister Paris 433 115 904)	Hosting der Plattform, der KI-Modelle für KI-Erkennung und Vorprüfung sowie der inhaltsbasierten Speicherung im Asset Management: verwaltetes Kubernetes, Load Balancer, privates Netzwerk, Messaging, Key Manager, Secret Manager, Objektspeicher	Frankreich, Rechenzentren im Großraum Paris	Verarbeitung ausschließlich in der EU, keine Drittlandübermittlung; weitere Rechenzentrumsbetreiber laut www.scaleway.com/en/subprocessorlist

Anhang 2: Technische und organisatorische Maßnahmen

Stand: November 2026. Der Auftragnehmer betreibt die Plattform, seine KI-Modelle und die Speicherknoten ausschließlich in Rechenzentren von Scaleway im Großraum Paris (Anhang 1), ohne Übermittlung in Drittstaaten. Die physische Sicherheit der Rechenzentren gewährleistet Scaleway über ein nach ISO/IEC 27001:2022 zertifiziertes Informationssicherheits-Managementsystem.

Organisation (Art. 32 Abs. 1 lit. b und d DSGVO)

Verantwortlichkeiten: Festlegung verbindlicher Zuständigkeiten für Informationssicherheit und Datenschutz; von der Geschäftsführung freigegebene Sicherheitsleitlinie; dokumentierte Eskalations- und Meldewege für Sicherheitsvorfälle.

Personal: Verpflichtung aller Beschäftigten auf Vertraulichkeit; Schulung zu Datenschutz und Informationssicherheit bei Eintritt und mindestens jährlich, einschließlich der Abwehr von Phishing und Social Engineering; geregelter Ein- und Austrittsprozess mit Vergabe und Entzug von Berechtigungen.

Verschlüsselung und Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Ruhende Daten: verschlüsselte Ablage gespeicherter Dateien in den Speicherknoten; Zugriff nur über das Zugriffstoken des jeweiligen Auftraggebers; Speicherung der Schlüssel getrennt von den Daten.

Schlüsselverwaltung: Verwaltung von Zugangsdaten im Secret Manager und von Signaturschlüsseln im Key Manager von Scaleway; Übergabe der Zugangsdaten an die Dienste erst beim Start und nur über TLS; Signaturvorgänge, auch für Content Credentials, ausschließlich über den Key Manager.

Externe Verbindungen: TLS 1.3 und TLS 1.2 als Mindestversion, TLS 1.0 und 1.1 werden abgelehnt; bei TLS 1.2 ausschließlich ECDHE-Schlüsselaustausch mit AEAD-Verfahren (AES-GCM, ChaCha20-Poly1305) und damit Perfect Forward Secrecy; Terminierung erst am Ingress im Cluster, der Load Balancer leitet den verschlüsselten Datenverkehr unverändert durch; Zertifikate von Let's Encrypt mit automatischer Erneuerung; HSTS für Webzugriffe.

Interne Verbindungen: Kommunikation der Dienste überwiegend asynchron über den Messaging-Dienst von Scaleway, je Dienst mit eigenen Zugangsdaten und über TLS; Verschlüsselung des Datenverkehrs zwischen den Knoten des Clusters mit WireGuard; Verbindungen zu Key Manager, Secret Manager und Objektspeicher ausschließlich über TLS; keine unverschlüsselten Protokolle.

Kryptografie: Einsatz anerkannter Algorithmen nach dem Stand der Technik, etwa AES-256 und SHA-256 oder stärker; keine Algorithmen mit bekannten Schwächen wie MD5, SHA-1 oder DES; regelmäßige Überprüfung der eingesetzten Algorithmen.

Blockchain:	Speicherung ausschließlich von Hashwerten und technischen Kennungen, keine Inhalte (Ziffer 7.4).
Pseudonymisierung:	interne Referenzierung von Dateien über zufällige oder inhaltsbasierte Kennungen.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle:	Verzicht auf eigene Serverräume; Betrieb ausschließlich in den zertifizierten Rechenzentren von Scaleway.
Zugangskontrolle:	Zugang zu administrativen Funktionen nur mit Mehr-Faktor-Authentifizierung und Schlüsselpaaren, ohne Anmeldung per Passwort; Betrieb des Clusters in einem privaten Netzwerk (Scaleway VPC) ohne gemeinsames Netzsegment mit anderen Kunden; Kerndienste und Speicherknoten ohne öffentlichen Zugang; standardmäßig sperrende Netzwerkrichtlinien im Cluster; Härtung der Server und Abschaltung nicht benötigter Dienste.
Nutzerkonten:	persönliche Kennungen ohne Gruppenkonten; passwortlose Anmeldung über Social Login oder Einmalcode per E-Mail, jeweils mit Mehr-Faktor-Authentifizierung; keine Speicherung von Passwörtern beim Auftragnehmer.
Zugriffskontrolle:	Rollen- und Berechtigungskonzept nach dem Erforderlichkeitsprinzip; getrennte Administrations- und Nutzerkennungen; keine Arbeit mit Root-Konten im Regelbetrieb; Überprüfung der Berechtigungen mindestens jährlich; Zugriff von Beschäftigten auf Inhalte des Auftraggebers nur, soweit für Support oder Störungsbehebung erforderlich, und dokumentiert.
Trennungskontrolle:	Mandantentrennung je Auftraggeber; getrennte Produktiv-, Test- und Entwicklungsumgebungen; keine Verarbeitung von Inhalten des Auftraggebers in Test- oder Entwicklungsumgebungen und kein Training von KI-Modellen mit diesen Inhalten.
Endgeräte:	Verschlüsselung der Datenträger, automatische Bildschirmsperre, Schutz vor Schadsoftware und automatische Sicherheitsupdates auf allen dienstlichen Endgeräten; keine Speicherung von Inhalten des Auftraggebers auf Endgeräten; Verlustmeldung und Fernlöschung mobiler Geräte.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle:	Betrieb der Speicherknoten als privates Netzwerk mit 256-Bit-Netzwerkschlüssel, ohne Verbindung zu öffentlichen Speichernetzwerken und ohne öffentliches Gateway; Abruf von Dateien nur authentifiziert und verschlüsselt; öffentliche Nachweise nur mit den vom Auftraggeber freigegebenen Angaben.
API und MCP-Server:	Zugriff nur mit persönlichen API-Schlüsseln; Begrenzung der Anfragen je Schlüssel; Widerruf von Schlüsseln im Konto.
Eingabekontrolle:	Nachvollziehbarkeit, wer welche Datei wann hochgeladen, gekennzeichnet oder gelöscht hat; Integritätsnachweis durch Hashwerte, Signatur der Content Credentials und Verankerung auf der Blockchain.
Inhaltsbasierte Speicherung:	Referenzierung jeder Datei im Asset Management über ihren Hashwert statt über Ordner und Dateinamen, sodass jede Veränderung erkennbar ist.
Protokollierung:	Erfassung administrativer Anmeldungen und Zugriffe auf die Infrastruktur im Audit Trail von Scaleway; Nutzung der Protokolle nur zu Sicherheits- und Nachweiszwecken.

Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Redundanz:	Speicherung jeder gespeicherten Datei auf mehreren Speicherknoten in getrennten Verfügbarkeitszonen.
Datensicherung:	Sicherung nach einem dokumentierten Konzept; verschlüsselte Sicherungskopien an einem räumlich getrennten Standort; mindestens eine Sicherung unveränderlich oder vom Produktivsystem getrennt (Schutz vor Ransomware); regelmäßige Wiederherstellungstests.
Notfallmanagement:	Notfall- und Wiederanlaufplan einschließlich der Szenarien Ransomware und Ausfall des Infrastrukturanbieters; regelmäßige Übungen; dokumentierte Ausstiegsstrategie für einen Anbieterwechsel.
Betrieb:	Überwachung der Systeme mit Alarmierung; Patch-Management mit unverzüglichem Einspielen kritischer Sicherheitsupdates; DDoS-Schutz durch Scaleway.

Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Überprüfung:	Prüfung und Anpassung dieser Maßnahmen mindestens jährlich und bei wesentlichen Änderungen; regelmäßige Schwachstellenprüfungen und Penetrationstests.
Entwicklung:	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO); Code-Reviews; automatisierte Prüfung von Code und Abhängigkeiten auf Schwachstellen; Inventarisierung der eingesetzten Komponenten; keine Zugangsdaten in der eigenen Quellcodeverwaltung; Sicherheitstests nach anerkannten Methoden, etwa des Open Worldwide Application Security Project (OWASP).
Sicherheitsvorfälle:	Verfahren zur Erkennung, Bewertung und Meldung von Sicherheitsvorfällen mit Information des Auftraggebers nach Ziffer 5.4; Dokumentation jedes Vorfalls.
Auftragskontrolle:	Einsatz von Unterauftragsverarbeitern nur nach Anhang 1, auf Grundlage eines Vertrags nach Art. 28 DSGVO und dokumentierter Garantien, insbesondere ISO/IEC 27001; jährliche Überprüfung anhand aktueller Zertifikate; Überwachung von Änderungen der Unterauftragsverarbeiter von Scaleway; kein administrativer Zugang externer Dienstleister zu den Systemen des Auftragnehmers; Dokumentation der Weisungen.
Löschung:	Aufhebung der Fixierung (Unpinning) und Bereinigung (Garbage Collection) auf allen Speicherknoten sowie Löschung der zugehörigen Schlüssel und Zuordnungsdaten; Deaktivierung zugehöriger Zugriffstoken und öffentlicher Nachweise; Sicherungskopien nach Ziffer 9.3; Bestätigung der Löschung in Textform auf Anfrage.