Vereinbarung zur Auftragsverarbeitung

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Template-Version 2026-04 · gültig für Resistro Cloud Verträge ab 2026-04-22 · letzte Aktualisierung der Subunternehmerliste in Anlage 2: 2026-04-22

Hinweis: Dieses Dokument ist ein Standard-Template. Es bildet die tatsächliche technische und organisatorische Realität von Resistro Cloud ab, ist aber **keine Rechtsberatung**. Bitte lassen Sie den Vertragstext vor Unterzeichnung durch Ihre Datenschutzbeauftragte oder einen Rechtsanwalt prüfen. Änderungswünsche besprechen wir gerne — schreiben Sie an *privacy@resistro.org*.

Zwischen

Auftraggeber (im Folgenden „Verantwortlicher"):

Firma: _____
Anschrift: _____
Vertreten durch: _____
USt-IdNr.: _____

und

Auftragnehmer (im Folgenden „Auftragsverarbeiter"):

Alexander Renz
Jahnstraße 13
82152 Krailling
Deutschland
E-Mail: privacy@resistro.org

— gemeinsam die „Parteien" —

Präambel

Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Rahmen des Dienstes „Resistro Cloud" (im Folgenden „Dienst"): verschlüsselte Aufbewahrung und Überwachung von Datenbank-Backups. Bei der Erbringung des Dienstes kann der Auftragsverarbeiter personenbezogene Daten verarbeiten, die der Verantwortliche in seinen Datenbanken sichert. Diese Vereinbarung regelt die Rechte und Pflichten der Parteien nach Art. 28 DSGVO.

Inhaltsverzeichnis

1. Gegenstand und Dauer des Auftrags
2. Art und Zweck der Datenverarbeitung, Art der Daten, Kategorien Betroffener
3. Pflichten des Auftragsverarbeiters
4. Technisch-organisatorische Maßnahmen (siehe Anlage 1)
5. Unterauftragsverhältnisse (siehe Anlage 2)
6. Weisungsrecht des Verantwortlichen
7. Unterstützung bei Betroffenenrechten und Meldepflichten
8. Rückgabe und Löschung personenbezogener Daten
9. Kontroll- und Prüfrechte
10. Haftung
11. Schlussbestimmungen

§1 Gegenstand und Dauer

(1) Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen des zwischen den Parteien abgeschlossenen Nutzungsvertrags für Resistro Cloud (im Folgenden „Hauptvertrag").

(2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Ein Kündigungsrecht bleibt hiervon unberührt.

§2 Art und Zweck der Datenverarbeitung, Art der Daten, Kategorien Betroffener

(1) **Art und Zweck** der Verarbeitung: Entgegennahme, Speicherung und Bereitstellung verschlüsselter Datenbank-Backups des Verantwortlichen; Überwachung der Backup-Ausführung; Bereitstellung einer Web-Oberfläche und API zur Verwaltung.

(2) **Art der personenbezogenen Daten:** abhängig vom Inhalt der vom Verantwortlichen gesicherten Datenbanken. Die Daten liegen beim Auftragsverarbeiter ausschließlich als AES-256-verschlüsselter Ciphertext vor; der Schlüssel verbleibt beim Verantwortlichen. Unverschlüsselt verarbeitet werden lediglich Metadaten zum Backup (Zeitstempel, Größe, Prüfsummen, Fehlermeldungen), Kontaktdaten des Verantwortlichen (Name, E-Mail), Agent-Hostnamen und IP-Adressen der zugreifenden Systeme.

(3) **Kategorien Betroffener:** Nutzer und Kunden des Verantwortlichen, deren Daten in den gesicherten Datenbanken enthalten sind, sowie Mitarbeitende des Verantwortlichen, die den Dienst bedienen.

(4) Verarbeitungsort ist das Gebiet der Europäischen Union. Eine Drittlandübermittlung findet nicht statt, es sei denn der Verantwortliche weist dies explizit an.

§3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Verantwortlichen.

(2) Der Auftragsverarbeiter verpflichtet seine mit der Verarbeitung befassten Personen zur Vertraulichkeit und unterrichtet sie über die datenschutzrechtlichen Pflichten.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung seiner Pflichten aus Art. 32–36 DSGVO (technische und organisatorische Maßnahmen, Meldepflichten, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(4) Sofern es gesetzlich vorgeschrieben ist, wird der Auftragsverarbeiter einen Datenschutzbeauftragten benennen. Derzeit besteht keine gesetzliche Benennungspflicht. Aktueller Ansprechpartner für Datenschutzfragen: *privacy@resistro.org*.

(5) Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich informieren, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt.

§4 Technisch-organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die in **Anlage 1** dokumentierten technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO. Diese sind so zu gestalten, dass das Schutzniveau dem Risiko angemessen ist.

Der Auftragsverarbeiter behält sich vor, die Maßnahmen weiterzuentwickeln, solange das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dem Verantwortlichen mit mindestens 30 Tagen Vorlauf mitgeteilt.

§5 Unterauftragsverhältnisse

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die **allgemeine schriftliche Genehmigung**, die in **Anlage 2** aufgeführten Unterauftragsverarbeiter zu beauftragen.

(2) Vor dem Hinzuziehen oder der Ersetzung eines Unterauftragsverarbeiters informiert der Auftragsverarbeiter den Verantwortlichen mit einer Vorlauffrist von mindestens 30 Tagen per E-Mail und im Dashboard. Der Verantwortliche kann dieser Änderung innerhalb der Frist aus wichtigem Grund widersprechen. Im Falle eines Widerspruchs sind beide Parteien zur außerordentlichen Kündigung des Hauptvertrags berechtigt.

(3) Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag ab, der diesem mindestens die gleichen datenschutzrechtlichen Verpflichtungen auferlegt, die dem Auftragsverarbeiter nach dieser Vereinbarung obliegen.

(4) Nicht als Unterauftragsverhältnis im Sinne dieses Paragraphen gelten Nebenleistungen (z.B. Telekommunikation, Entsorgung von Datenträgern, Reinigung), die der Auftragsverarbeiter von Dritten in Anspruch nimmt, soweit diese keinen Zugriff auf personenbezogene Daten haben.

§6 Weisungsrecht des Verantwortlichen

(1) Der Verantwortliche erteilt alle Weisungen schriftlich (E-Mail an *privacy@resistro.org* genügt). Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(2) Weisungsberechtigt auf Seiten des Verantwortlichen sind die in der Dashboard-Kontoverwaltung hinterlegten administrativen Ansprechpartner.

(3) Der Auftragsverarbeiter wird Weisungen nur im Rahmen dieses Vertrags und im Rahmen des technisch und rechtlich Möglichen umsetzen.

§7 Unterstützung bei Betroffenenrechten und Meldepflichten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen soweit möglich bei der Beantwortung von Anträgen betroffener Personen (Art. 15–22 DSGVO) und bei Meldungen an die Aufsichtsbehörde (Art. 33 DSGVO) bzw. Benachrichtigungen betroffener Personen (Art. 34 DSGVO).

(2) Der Auftragsverarbeiter informiert den Verantwortlichen **unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis** über personenbezogene Datenschutzverletzungen in seinem Verantwortungsbereich.

§8 Rückgabe und Löschung personenbezogener Daten

(1) Nach Beendigung des Hauptvertrags werden sämtliche personenbezogenen Daten des Verantwortlichen, einschließlich aller Backup-Objekte, innerhalb von **30 Tagen** unwiederbringlich gelöscht. Der Verantwortliche kann innerhalb dieser Frist verlangen, die Daten zuvor an ihn zurückzugeben.

(2) Metadaten für gesetzliche Aufbewahrungsfristen (insbesondere Rechnungsdaten nach §147 AO) werden bis zum Ende der jeweiligen Frist aufbewahrt.

(3) Die Löschung wird dem Verantwortlichen auf Anforderung schriftlich bestätigt.

§9 Kontroll- und Prüfrechte

(1) Der Verantwortliche hat das Recht, die Einhaltung der Vorschriften über den Datenschutz und die technisch-organisatorischen Maßnahmen zu prüfen.

(2) Prüfungen erfolgen nach Ankündigung mit angemessener Frist (mindestens 14 Tage) während der üblichen Geschäftszeiten und ohne Beeinträchtigung des Betriebsablaufs.

(3) Der Auftragsverarbeiter kann Prüfungen durch Vorlage geeigneter Nachweise (aktueller Stand der Anlage 1, Prüfberichte externer Auditoren sofern vorhanden, schriftliche Bestätigungen) ersetzen, soweit der Verantwortliche dem zustimmt.

(4) Der angemessene Mehraufwand des Auftragsverarbeiters für eine Prüfung kann nach Stundensatz berechnet werden, sofern die Prüfung nicht anlassbezogen (bei Datenschutzvorfällen, auf behördliche Aufforderung) stattfindet.

§10 Haftung

Die Haftung zwischen den Parteien richtet sich nach dem Hauptvertrag. Art. 82 DSGVO bleibt unberührt. Eine gesamtschuldnerische Haftung beider Parteien gegenüber Betroffenen besteht nach Art. 82 Abs. 4 DSGVO; der interne Ausgleich erfolgt nach Verursachungsbeiträgen.

§11 Schlussbestimmungen

(1) Für Nebenabreden ist die Schriftform erforderlich; E-Mail genügt.

(2) Es gilt deutsches Recht. Ausschließlicher Gerichtsstand ist, soweit zulässig, München.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

(4) Bei Widersprüchen zwischen dem Hauptvertrag und dieser Vereinbarung geht diese Vereinbarung vor, soweit datenschutzrechtliche Fragen betroffen sind.

Ort, Datum Unterschrift Verantwortlicher

Ort, Datum Unterschrift Auftragsverarbeiter

Anlage 1: Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

Stand: 2026-04-22. Der Auftragsverarbeiter behält sich vor, die Maßnahmen weiterzuentwickeln, solange das Schutzniveau insgesamt nicht unterschritten wird.

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

Kategorie	Maßnahme
Zutrittskontrolle	Rechenzentrum der Hetzner Online GmbH (Nürnberg). ISO 27001-zertifizierter Betrieb, 24/7 personal security, Biometrie, Videoüberwachung, RFID-Zutrittskontrollen. Nachgewiesen durch Hetzner-ISO-Zertifikat.
Zugangskontrolle	Ausschließlich SSH-Key-basierter Zugang zu Produktivsystemen. 2FA auf Management-Oberflächen. Keine statischen Passwörter für Admin-Zugänge. Zugriff auf Kundendaten ist auf den Geschäftsinhaber und explizit beauftragte, schriftlich zur Vertraulichkeit verpflichtete Mitarbeitende oder Unterauftragsverarbeiter beschränkt; jede Erweiterung erfolgt schriftlich dokumentiert.
Zugriffskontrolle (logisch)	Mandantenisolation auf SQL-Ebene durch `tenant_id`-Scoping in jeder Abfrage. Separate Prefix-Partitionierung im Object-Storage pro Mandant. API-Key pro Mandant, widerrufbar.
Trennungskontrolle	Produktions-, Staging- und Entwicklungsdaten sind getrennt. Jeder Backup-Datensatz ist mit `tenant_id` und individuellem Verschlüsselungs-Schlüssel gebunden.
Pseudonymisierung / Verschlüsselung	Backup-Inhalte sind AES-256-CTR-verschlüsselt *vor* Übertragung zum Auftragsverarbeiter. Der Schlüssel verbleibt beim Verantwortlichen. Der Auftragsverarbeiter speichert nur einen SHA-256-Fingerprint zur Schlüsselprüfung. Transportverschlüsselung: TLS 1.2+.

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

Kategorie	Maßnahme
Weitergabekontrolle	Alle API-Verbindungen über HTTPS (TLS 1.2+). Backup-Upload erfolgt als verschlüsseltes Multipart-PUT. Keine Datenweitergabe an Dritte außerhalb der genehmigten Unterauftragsverhältnisse.
Eingabekontrolle	Protokollierung von Admin-Zugriffen, API-Zugriffen (Methode, Pfad, Status, Zeitstempel, Quell-IP). Kein Logging von API-Keys oder Request-Bodies. Log-Retention 30 Tage.

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

Kategorie	Maßnahme
Verfügbarkeit	Redundante Stromversorgung und Internetanbindung im Rechenzentrum Hetzner Nürnberg. SLA-Ziel des Dienstes: 99,9 % Verfügbarkeit pro Monat (Enterprise-Tier).
Belastbarkeit	

	Rate-Limits pro Mandant gegen Überlastung einzelner Komponenten. Quota-Enforcement pro Mandant verhindert Ressourcen-Monopolisierung.
Wiederherstellung	Metadaten-Datenbank wird selbst via resistro gesichert (Dogfood). Object-Storage-Backup-Daten liegen in Hetzner-Objekt-Speicher mit redundanten Kopien. Wiederherstellungstests werden regelmäßig durchgeführt; Ergebnisse werden intern dokumentiert und auf Anforderung dem Verantwortlichen vorgelegt.

4. Regelmäßige Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Kategorie	Maßnahme
Datenschutz-Management	Überprüfung der TOMs mindestens jährlich. Unmittelbare Anpassung bei Sicherheitsereignissen.
Incident-Response	Security-Kontakt: *security@resistro.org*. Meldekette zum Verantwortlichen <24h nach Kenntnis gemäß §7 Abs. 2 dieses Vertrags.
Auftragskontrolle	Unterauftragsverarbeiter (Anlage 2) werden nur mit vorheriger allgemeiner Genehmigung und Information des Verantwortlichen eingesetzt.

Anlage 2: Unterauftragsverarbeiter

Stand: 2026-04-22. Änderungen werden mit mindestens 30 Tagen Vorlauf angekündigt (§5 Abs. 2 dieses Vertrags).

Unterauftragsverarbeiter	Anschrift / Land	Zweck und Art der Datenverarbeitung	Betroffene Datenkategorien
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Cloud-Server (Compute), Hosting der Metadaten-Datenbank	Account-Daten, Backup-Metadaten, Server-Logs
Hetzner Online GmbH (Object Storage)	Rechenzentrum Nürnberg (nbg1), Deutschland	Objektspeicher für verschlüsselte Backup-Dateien	Ausschließlich AES-256-Ciphertext
Paddle.com Market Ltd.	Judd House, 18–29 Mora Street, London EC1V 8BT, UK / Paddle.com Inc. (Delaware) als Merchant-of-Record	Zahlungsabwicklung, Rechnungsstellung, Umsatzsteuerabwicklung	Name, E-Mail, Rechnungsanschrift, Zahlungsdaten des Verantwortlichen (nicht der Betroffenen)

Hetzner stellt einen AVV nach Art. 28 DSGVO bereit; der Auftragsverarbeiter hat diesen geschlossen. Paddle fungiert als Merchant-of-Record in eigenem Vertragsverhältnis mit dem Endkunden (vgl. Paddle Standard Contractual Clauses).