VERIST

Auftragsverarbeitungsvereinbarung (AVV)

Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DSGVO

Stand: 28. April 2026 **Version:** 1.0 **Vorlage:** Standard-Template **Geltungsbereich:** VERIST-Plattform (verist.de)

Hinweis zur Verwendung dieser Vorlage. Diese Auftragsverarbeitungsvereinbarung ist eine Standard-Vorlage der EXTRA Group GmbH und stellt keine individuelle Rechtsberatung dar. Sie deckt die Pflichtinhalte nach Art. 28 DSGVO vollständig ab und kann im Vertragsprozess durch die Rechtsabteilung des Auftraggebers individuell verhandelt und angepasst werden. Maßgeblich ist die im Vertragsschluss unterzeichnete und von beiden Parteien gegengezeichnete Fassung. Die Geltung dieser Vorlage allein begründet keine vertragliche Bindung; sie dient ausschließlich der Vorbereitung und Transparenz im Beschaffungsprozess.

VERANTWORTLICHER (AUFTRAGGEBER)

[Firmenname Auftraggeber]
[Anschrift]
[Postleitzahl, Stadt]
[Vertretungsberechtigte/-r]

— nachfolgend „Verantwortlicher" —

AUFTRAGSVERARBEITER

EXTRA Group GmbH
Mathes-Deutsch-Weg 24B
D-84036 Landshut
Vertreten durch: die Geschäftsführung

HRB 8523 · USt-IdNr. DE 277 654 355

— nachfolgend „Auftragsverarbeiter" —

Der Verantwortliche und der Auftragsverarbeiter (gemeinsam „Parteien") schließen die nachfolgende Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag, die im Rahmen der Nutzung der VERIST-Plattform durch den Verantwortlichen erfolgt. Diese Vereinbarung ergänzt den Hauptvertrag (Lizenz-, Service- oder Bestellvereinbarung) zwischen den Parteien.

§ 1 Gegenstand und Zweck der Verarbeitung

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Rahmen der Bereitstellung und des Betriebs der VERIST-Plattform für den Verantwortlichen. Die Plattform dient der Inventarisierung, Risikoklassifizierung und revisionssicheren Dokumentation von KI-Systemen des Verantwortlichen im Sinne der Verordnung (EU) 2024/1689 (KI-Verordnung / EU AI Act).

Zweck der Verarbeitung ist ausschließlich die Erfüllung der vertraglich geschuldeten Leistungen des Auftragsverarbeiters gegenüber dem Verantwortlichen. Eine Verarbeitung zu eigenen Zwecken des Auftragsverarbeiters erfolgt nicht.

Art und Kategorien der personenbezogenen Daten sowie der betroffenen Personen sind in **Anhang A** beschrieben.

§ 2 Art, Umfang und Mittel der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dies gilt insbesondere für Übermittlungen von Daten an ein Drittland oder eine internationale Organisation. Eine solche Verarbeitung findet nicht statt, soweit nicht der Auftragsverarbeiter durch das Recht der Europäischen Union oder eines Mitgliedstaats verpflichtet ist; in diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen die rechtlichen Anforderungen vorab mit, sofern das jeweilige Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Die Verarbeitung erfolgt ausschließlich innerhalb der Europäischen Union, insbesondere am Hosting-Standort Frankfurt am Main, Deutschland. Eine Übermittlung in Drittländer ist ausgeschlossen, soweit nicht ausdrücklich vom Verantwortlichen genehmigt und durch geeignete Garantien nach Art. 46 ff. DSGVO abgesichert.

Die Mittel der Verarbeitung umfassen insbesondere: Speicherung in der GRAVITY-Datenbank (Supabase, Frankfurt), Verarbeitung auf Anwendungs-Servern (Hetzner, Frankfurt), Object-Storage (MinIO, Hetzner), kryptographische Hash-Chain für Decision Records, transaktionale E-Mail-Versand (Strato, Deutschland) und Zahlungsabwicklung über Stripe Payments Europe Ltd. (Dublin, Irland) für innereuropäische Zahlungen.

§ 3 Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter wird die ihm überlassenen personenbezogenen Daten ausschließlich entsprechend dieser Vereinbarung und den Weisungen des Verantwortlichen verarbeiten. Er ist insbesondere verpflichtet:

1. die personenbezogenen Daten ausschließlich zu den vereinbarten Zwecken zu verarbeiten;
2. sicherzustellen, dass alle zur Verarbeitung der personenbezogenen Daten befugten Personen sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. die zur Sicherheit der Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO zu treffen (siehe **Anhang B**);
4. die Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters nach **§ 5** dieser Vereinbarung einzuhalten;
5. den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß Art. 32 bis 36 DSGVO zu unterstützen, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Datenschutzverletzungen und der Datenschutz-Folgenabschätzung;
6. nach Wahl des Verantwortlichen alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen zu löschen oder zurückzugeben;
7. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen einschließlich Inspektionen zu ermöglichen.

§ 4 Mitwirkungspflichten und Hilfeleistungen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Beantwortung von Anträgen betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO.

Insbesondere stellt der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen bereit, um den Verantwortlichen bei folgenden Pflichten zu unterstützen:

- Auskunftsrecht der betroffenen Person (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung („Recht auf Vergessenwerden", Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)

Anfragen, die direkt beim Auftragsverarbeiter eingehen, leitet dieser unverzüglich an den Verantwortlichen weiter.

Der Auftragsverarbeiter benennt eine Kontaktstelle für Datenschutzanfragen: **datenschutz@verist.de**.

§ 5 Subunternehmer (Subprozessoren)

Der Verantwortliche genehmigt mit Abschluss dieser Vereinbarung allgemein die Hinzuziehung von Subprozessoren durch den Auftragsverarbeiter zur Erbringung der vertraglichen Leistungen. Eine aktuelle Liste der eingesetzten Subprozessoren ist in **Anhang C** sowie öffentlich auf verist.de/trust#subprozessoren einsehbar.

Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter (Subprozessoren) **30 Tage** vor der geplanten Änderung schriftlich oder per E-Mail. Der Verantwortliche kann gegen die Änderung Einspruch erheben.

Bei jeder Hinzuziehung eines Subprozessors stellt der Auftragsverarbeiter sicher, dass dieser:

- einer schriftlichen Vereinbarung unterliegt, die im Wesentlichen dieselben Datenschutzpflichten wie diese Vereinbarung enthält;
- geeignete technische und organisatorische Maßnahmen zur Einhaltung der DSGVO trifft;
- die personenbezogenen Daten ausschließlich innerhalb der Europäischen Union verarbeitet, soweit nicht ausdrücklich anders vereinbart.

Kommt der Subprozessor seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subprozessors.

§ 6 Technisch-organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die jeweils aktuellen TOMs des Auftragsverarbeiters sind in **Anhang B** sowie öffentlich auf verist.de/trust#toms einsehbar.

Wesentliche Bestandteile sind:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten (TLS 1.3 in-transit, AES-256 at-rest);
- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme (Hash-Chain für Audit-Logs, geo-redundantes Backup);
- Verfahren zur raschen Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs nach physischem oder technischem Vorfall (RTO ≤ 4h, RPO ≤ 24h);
- regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs (kontinuierliches ISMS-Monitoring, quartalsweise Restore-Tests).

Änderungen an den TOMs sind zulässig, soweit sie das vereinbarte Schutzniveau nicht unterschreiten. Wesentliche Änderungen werden dem Verantwortlichen mitgeteilt.

§ 7 Auskunfts- und Mitwirkungspflichten gegenüber Aufsichtsbehörden

Der Auftragsverarbeiter wirkt mit der zuständigen Aufsichtsbehörde des Verantwortlichen auf Anfrage bei der Erfüllung ihrer Aufgaben zusammen.

Im Falle einer behördlichen Anordnung oder Maßnahme im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, es sei denn, das geltende Recht verbietet eine solche Mitteilung.

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung seiner Auskunftspflichten gegenüber der Aufsichtsbehörde, insbesondere durch Bereitstellung der zur Verarbeitung relevanten Informationen, Audit-Logs und Decision Records.

§ 8 Meldung von Datenschutzverletzungen

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, die sich auf Daten des Verantwortlichen bezieht, so meldet er diese dem Verantwortlichen unverzüglich, spätestens jedoch innerhalb von **24 Stunden** nach Kenntniserlangung.

Die Meldung enthält mindestens:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2. den Namen und die Kontaktdaten der Kontaktstelle des Auftragsverarbeiters, bei der weitere Informationen erlangt werden können;
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
4. eine Beschreibung der vom Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragsverarbeiter führt ein Verzeichnis aller Datenschutzverletzungen mit Hash-Chain-Eintrag (manipulationssicher) und stellt es dem Verantwortlichen auf Anfrage zur Verfügung.

Sicherheitsvorfälle können auch direkt an **security@verist.de** gemeldet werden.

§ 9 Rückgabe und Löschung der Daten

Nach Abschluss der Erbringung der vertraglichen Leistungen, spätestens jedoch nach Beendigung dieser Vereinbarung oder des Hauptvertrags, hat der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten:

1. an den Verantwortlichen zurückzugeben (in einem strukturierten, gängigen, maschinenlesbaren Format) oder
2. vollständig zu löschen.

Die Löschung umfasst auch alle vorhandenen Kopien der Daten in Backups. Aufgrund der Backup-Rotation kann die vollständige Löschung aus Backups bis zu 30 Tage dauern. Während dieser Zeit werden die Daten nicht aktiv verarbeitet.

Eine längere Aufbewahrung erfolgt nur, soweit gesetzliche Aufbewahrungspflichten (z. B. nach HGB §257, AO §147) eine Löschung nicht zulassen. Audit-Logs und Decision Records werden nach **§ 7** dieser Vereinbarung für die Dauer von 7 Jahren aufbewahrt.

Der Auftragsverarbeiter weist die Löschung auf Anforderung schriftlich nach.

§ 10 Vertragsdauer und Kündigung

Diese Vereinbarung beginnt mit dem im Hauptvertrag vereinbarten Zeitpunkt und endet automatisch mit dessen Beendigung.

Eine außerordentliche Kündigung dieser Vereinbarung durch den Verantwortlichen ist insbesondere möglich, wenn:

- der Auftragsverarbeiter wesentliche Pflichten dieser Vereinbarung trotz Abmahnung nicht einhält;
- der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführen kann oder will und keine alternative Lösung gefunden werden kann;
- der Auftragsverarbeiter den Zugriff der zuständigen Aufsichtsbehörde verweigert.

Im Falle einer Kündigung gelten die Pflichten nach **§ 9** (Rückgabe und Löschung) entsprechend.

§ 11 Haftung

Die Haftung der Parteien aus oder in Zusammenhang mit dieser Vereinbarung richtet sich nach den Bestimmungen der Datenschutz-Grundverordnung, insbesondere Art. 82 DSGVO, sowie nach den allgemeinen gesetzlichen Vorschriften.

Eine etwaige Haftungsbegrenzung im Hauptvertrag gilt entsprechend, sofern dies nach Art. 82 DSGVO und sonstigen zwingenden Rechtsvorschriften zulässig ist.

§ 12 Schlussbestimmungen

Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser Vereinbarung in Bezug auf die Datenverarbeitung vor.

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformklausel. Elektronische Signaturen nach eIDAS-Verordnung gelten der Schriftform als gleichwertig.

Sollte eine Bestimmung dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, so berührt dies nicht die Wirksamkeit der übrigen Bestimmungen. Anstelle der unwirksamen oder undurchführbaren Bestimmung gilt diejenige wirksame und durchführbare Regelung, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen.

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder in Zusammenhang mit dieser Vereinbarung ist Landshut, Deutschland, soweit der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

ANHANG A Kategorien personenbezogener Daten und betroffener Personen

Im Rahmen der Nutzung der VERIST-Plattform werden folgende Kategorien personenbezogener Daten verarbeitet:

KATEGORIE	DATENARTEN	BETROFFENE PERSONEN
Account-Stammdaten	Name, E-Mail-Adresse, Position, Telefonnummer (optional), Firmenzugehörigkeit	Mitarbeitende des Verantwortlichen mit Plattform-Zugang
Audit- & Aktivitätsdaten	Login-Zeitpunkte, IP-Adressen, durchgeführte Aktionen, Decision Records	Mitarbeitende des Verantwortlichen mit Plattform-Zugang
KI-System-Metadaten	Inventar-Einträge zu KI-Systemen, Risikoklassifizierungen, Compliance-Status	Verarbeitung kann sich indirekt auf betroffene Personen beziehen, deren Daten von den KI-Systemen des Verantwortlichen verarbeitet werden — diese Daten selbst werden nicht in der VERIST-Plattform gespeichert
Vertrags- & Abrechnungsdaten	Firmenname, Rechnungsanschrift, USt-IdNr., Zahlungsdaten (verarbeitet durch Stripe)	Vertragspartner, Buchhaltungs-Kontaktpersonen
Support-Kommunikation	E-Mail-Inhalte, Anhänge, Chat-Verläufe	Mitarbeitende des Verantwortlichen, die Support kontaktieren

Die Verarbeitung erfolgt für die Dauer der Nutzung der VERIST-Plattform durch den Verantwortlichen sowie für gesetzliche Aufbewahrungsfristen.

ANHANG B Technisch-organisatorische Maßnahmen (TOMs)

Die jeweils aktuelle Fassung der TOMs ist im VERIST Trust Center öffentlich einsehbar:
verist.de/trust#toms

Die TOMs umfassen mindestens:

1. **Zugangskontrolle:** ISO-27001-zertifiziertes Hetzner-Rechenzentrum, SSH-Schlüssel-basierter Zugang (Ed25519, kein Passwort-Login)
2. **Zugriffskontrolle:** Rollenbasiertes Berechtigungsmodell, Bearer-Token-Authentifizierung mit 30-Min-TTL
3. **Eingabekontrolle:** Manipulationssichere Hash-Chain (SHA-256) für alle datenverändernden Aktionen
4. **Auftragskontrolle:** Vollständige Subprozessoren-Dokumentation, DSGVO-Art-28-Vereinbarungen mit allen Subprozessoren
5. **Verfügbarkeitskontrolle:** Tägliche Backups, 30 Tage Retention, RTO ≤ 4h, RPO ≤ 24h, Monitoring mit Eskalation
6. **Trennungskontrolle:** Mandantentrennung auf Datenbank-Ebene, Row-Level-Security
7. **Pseudonymisierung:** UUIDs als interne Schlüssel, minimierte Klartext-PII
8. **Verschlüsselung:** TLS 1.3 in-transit, AES-256 at-rest, SHA-256 für Hash-Chain
9. **Wiederherstellbarkeit:** Dokumentierter Disaster-Recovery-Prozess, quartalsweise Restore-Verifikation

Wesentliche Änderungen der TOMs werden dem Verantwortlichen mitgeteilt, soweit sie das vereinbarte Schutzniveau betreffen.

ANHANG C Genehmigte Subprozessoren

Die jeweils aktuelle Fassung der Subprozessoren-Liste ist im VERIST Trust Center öffentlich einsehbar:
verist.de/trust#subprozessoren
Stand bei Vertragsschluss (28.04.2026):

ANBIETER	STANDORT	ZWECK	VERTRAGSBASIS
Hetzner Online GmbH	Frankfurt am Main, Deutschland	Hosting, Object-Storage	DSGVO Art. 28 · ISO 27001
Supabase Inc.	Frankfurt (eu-central-1)	Datenbank, Auth	DSGVO Art. 28 · SOC 2 Type II
Stripe Payments Europe Ltd.	Dublin, Irland (innereuropäisch)	Zahlungsabwicklung	DSGVO Art. 28 · PCI DSS Level 1
Strato AG	Berlin / Karlsruhe, Deutschland	Transaktionaler E-Mail-Versand	DSGVO Art. 28

Änderungsmeldung: Über beabsichtigte Änderungen wird der Verantwortliche mit einer Vorlauffrist von **30 Tagen** per E-Mail informiert. Einsprüche sind innerhalb dieser Frist möglich.

Im Vertragsprozess ergänzen. Diese Standard-Vorlage wird im Vertragsprozess durch die individuell verhandelten Bestimmungen vervollständigt und von beiden Parteien gegengezeichnet.

Verantwortlicher
Ort, Datum · Unterschrift

Auftragsverarbeiter
EXTRA Group GmbH · Geschäftsführung
Ort, Datum · Unterschrift