Auftragsverarbeitungsvertrag

Vertrag zur Auftragsverarbeitung der Rev2 Innovations GmbH nach Art. 28 DSGVO. Stand 18.05.2026.

Art. 28 DSGVO stellt spezifische Anforderungen an eine Auftragsverarbeitung. Zur Wahrung dieser speziellen Anforderungen schließen die Vertragsparteien zusätzlich zu den Allgemeinen Geschäftsbedingungen (AGB) bzw. dem Hauptvertrag diesen Vertrag zur Auftragsverarbeitung. Er findet Anwendung auf alle Tätigkeiten, die mit dem abgeschlossenen Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers, oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachstehend „Daten“) des Auftraggebers verarbeiten. Es gelten die Begriffsbestimmungen der DSGVO.

Mit Annahme eines Angebots der Rev2 Innovations GmbH bzw. mit Abschluss eines Hauptvertrages (Lizenzvertrag, Softwarevertrag oder Dienstleistungsvertrag) wird dieser Auftragsverarbeitungsvertrag in der jeweils auf rev2.at/avv veröffentlichten Fassung Vertragsbestandteil. Eine gesonderte Unterzeichnung ist nicht erforderlich.

Dieser Auftragsverarbeitungsvertrag bildet den allgemeinen Rahmen für alle von der Rev2 Innovations GmbH bereitgestellten Softwarelösungen. Die jeweils zutreffende Beschreibung der Verarbeitung sowie die Liste der eingesetzten Subauftragnehmer ergibt sich aus der modulspezifischen Anlage, die jedem Angebot beigefügt ist und integraler Bestandteil dieses Vertrages wird.

§ 1 Vertragsgegenstand und Weisungsrecht des Auftraggebers

(1) Gegenstand dieses Vertrages sind Leistungen des Auftragnehmers für den Auftraggeber im Bereich der Bereitstellung und des Betriebs der jeweils beauftragten Softwarelösungen sowie damit verbundener Dienstleistungen (Wartung, Support, Weiterentwicklung). Die konkrete Leistung ergibt sich aus dem Hauptvertrag sowie der modulspezifischen Anlage. Bei Änderungen der beauftragten Leistung ist die modulspezifische Anlage entsprechend anzupassen und zu ergänzen.

(2) **Dem Auftraggeber als verantwortliche Stelle obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung nach der DSGVO.**

(3) Bei der Erbringung der Leistung erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist.

(4) Die Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt und können vom Auftraggeber in zumindest dokumentiert elektronischem Format durch Einzelweisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten,

dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit (Art. 28 Abs. 3 lit. a DSGVO).

(5) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen, ohne dass ihm hierdurch negative Konsequenzen entstehen. Der Auftraggeber ist für die Erteilung rechtsgültiger Weisungen verantwortlich (Art. 28 Abs. 3 Satz 3 DSGVO).

(6) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 2 Technisch-organisatorische Maßnahmen

(7) Der Auftragnehmer beachtet die gesetzlichen Bestimmungen über den Datenschutz. Eine Weitergabe oder Offenlegung von Informationen des Auftraggebers an Dritte erfolgt ohne eine ausdrückliche Weisung des Auftraggebers nicht. Unterlagen und Daten werden gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik gesichert.

(8) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO getroffen hat. Hierzu wird auf Anlage 2 verwiesen.

(9) Der Auftraggeber überprüft vor der Aufnahme der Datenverarbeitung und sodann regelmäßig die technischen und organisatorischen Maßnahmen des Auftragnehmers. Änderungen an den vereinbarten Sicherheitsmaßnahmen können vorgenommen werden, soweit diese das vertraglich vereinbarte Schutzniveau nicht unterschreiten.

§ 3 Vertraulichkeit

Dem Auftragnehmer und dessen Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der Auftragnehmer verpflichtet alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden, zur Vertraulichkeit. Die Vertraulichkeitsverpflichtungen gelten auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer.

§ 4 Informationspflichten des Auftragnehmers

(10) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren, soweit sie sich auf diesen Vertrag beziehen. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen.

(11) Die Meldung über eine Verletzung des Schutzes personenbezogener Daten an den Auftraggeber enthält, soweit möglich, folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(12) Der Auftragnehmer trifft **unverzüglich** die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen, informiert den Auftraggeber und ersucht diesen um weitere Weisungen.

(13) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

(14) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 (Art. 28 Abs. 3 lit. e DSGVO) sowie Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO).

§ 5 Kontrollrechte des Auftraggebers

(15) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer

Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(16) Inspektionen durch den Auftraggeber bzw. dessen beauftragten Prüfern, die in keinem Wettbewerbsverhältnis zum Auftragnehmer stehen dürfen, können zu den üblichen Geschäftszeiten und mit einer Vorlaufzeit der Ankündigung von 14 Tagen durchgeführt werden. Der Auftraggeber führt Kontrollen nur im erforderlichen Umfang durch und stört Betriebsabläufe des Auftragnehmers dabei nur in verhältnismäßiger Weise. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Die Vergütung wird einzelvertraglich vereinbart.

§ 6 Einsatz von Subauftragnehmern

(17) Eine Verarbeitung personenbezogener Daten in Drittländern darf nur unter Einhaltung der Vorschriften der Art. 44 bis 49 DSGVO erfolgen. Die vertraglich vereinbarten Leistungen werden unter Hinzuziehung der in der modulspezifischen Anlage genannten Subauftragnehmer durchgeführt. Alle zum Vertragsschluss bereits hinzugezogenen und durch den Auftraggeber genehmigten weiteren Auftragsverarbeiter ergeben sich aus der jeweiligen Anlage. Der Auftraggeber erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten hinzuzuziehen. Wir haben die Verpflichtung, unsere Auftraggeber über die Hinzuziehung oder Änderung weiterer Auftragsverarbeiter zu informieren, wobei die Information schriftlich in Textform ausreichend ist. Weiters schließen wir mit sämtlichen Subauftragnehmern vergleichbare Verträge zur Auftragsverarbeitung ab. Wir unterrichten unsere Auftraggeber mindestens 14 Tage im Voraus in schriftlicher Form über alle beabsichtigten Änderungen der Subauftragnehmerliste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumen dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des betreffenden Unterauftragsverarbeiters Einwände gegen diese Änderungen erheben zu können (Einspruchsrecht nach Art. 28 Abs. 2 Satz 2 DSGVO). Das Einspruchsrecht erlischt, sofern Sie nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung über die Änderung oder Hinzuziehung schriftlich Einspruch erhoben haben. Im Falle eines Einspruchs besteht das beiderseitige Recht, den Hauptvertrag sowie diesen Vertrag zur Auftragsverarbeitung mit einer Frist von 3 Monaten zu kündigen.

(18) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die

auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 7 Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§ 8 Beendigung des Hauptvertrags

(19) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder, auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(20) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 9 Schlussbestimmungen

(21) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(22) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats.

(23) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt und es gelten die gesetzlichen Regelungen des Art. 28 DSGVO.

(24) Diese Vereinbarung unterliegt österreichischem Recht. Ausschließlicher Gerichtsstand ist Wien.

Anlagen:

- Anlage 1: Beschreibung der betroffenen Personen, Datenkategorien und Verarbeitungszwecke (modulspezifisch, separat)
- Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers
- Anlage 3: Genehmigte Subauftragnehmer (modulspezifisch, separat)

Anlage 2: Technische und organisatorische Maßnahmen (TOMs) der Rev2 Innovations GmbH gemäß Art. 32 DSGVO. Stand 18.05.2026.

Die Rev2 Innovations GmbH betreibt ihre Systeme im Rahmen eines Cloud-first- und Remote-first-Betriebsmodells. Die nachfolgenden technischen und organisatorischen Maßnahmen orientieren sich am Stand der Technik, an der Art, dem Umfang und den Risiken der Verarbeitung sowie an den Sicherheitsmaßnahmen der eingesetzten Cloud- und Plattformdienstleister. Physische Sicherheitsmaßnahmen zu Rechenzentren werden ausschließlich durch die eingesetzten Cloud-Anbieter umgesetzt.

1. Vertraulichkeit

a. Zutrittskontrolle (physisch)

- Rev2 betreibt keine eigenen Server- oder Rechenzentrumsräume.
- Physische Zutrittskontrollen wie Zugangssysteme, Videoüberwachung, Wachdienste und Brandschutz werden durch die eingesetzten Rechenzentrums- und Cloud-Anbieter umgesetzt.
- Die Auswahl der Anbieter erfolgt auf Basis dokumentierter Sicherheitsmaßnahmen und Zertifizierungen (ISO 27001 oder vergleichbar).
- Geschäftsräume in Wien sind durch Schließanlage gesichert.

b. Zugangskontrolle (Systemzugang)

- Personalisierte Benutzerkonten.
- Passwort-Richtlinien (Komplexität, Länge) und Passwort-Hashing nach aktuellem Stand der Technik.
- Mehrfaktor-Authentifizierung (MFA) für kritische Systeme, soweit technisch verfügbar.
- Einsatz eines Passwort-Managers im Unternehmen.
- Automatische Sperrung nach mehrfach fehlgeschlagenen Anmeldeversuchen.
- Automatische Bildschirmsperren.
- Clean-Desk- und Clear-Screen-Policy.
- Verschlüsselte Übertragung sämtlicher Anmeldedaten (TLS 1.2 oder höher).
- Zugriff ausschließlich über freigegebene Cloud-Dienste.

c. Zugriffskontrolle (Datenebene)

- Rollenbasiertes Berechtigungskonzept.
- Row-Level Security auf Datenbankebene.
- Strenges Need-to-know-Prinzip.
- Verwaltung von Berechtigungen durch autorisierte Administratoren.
- Reduktion administrativer Rechte auf das notwendige Minimum.
- Berücksichtigung von Zugriffsrechten auf Datensicherungen.
- Protokollierung administrativer Tätigkeiten.

2. Integrität

Gewährleistung der Richtigkeit, Integrität und Vollständigkeit personenbezogener Daten.

a. Eingabe- und Änderungsnachvollziehbarkeit

- Protokollierung von Erstellung, Änderung und Löschung personenbezogener Daten.
- Individuelle Benutzerkennungen (keine Sammelkonten).
- Absicherung und Integrität von Log- und Protokolldateien.
- Zeitstempel und Benutzerzuordnung bei allen Datenoperationen.

b. Übertragungskontrolle

- Datenübertragungen ausschließlich über verschlüsselte Kommunikationsverbindungen (TLS 1.2 oder höher). Physische Datentransporte finden nicht statt.
- Nutzung ausschließlich freigegebener Schnittstellen.
- Keine Speicherung sensibler Daten in URL-Parametern.

3. Verfügbarkeit und Belastbarkeit

- Betrieb auf einer hochverfügbaren Cloud-Infrastruktur.
- Nutzung redundanter Systemarchitekturen.
- Tägliche automatisierte Backups der Datenbank.
- Geografisch verteilte Speicherung von Sicherungen.
- Regelmäßige Tests der Datenwiederherstellung.
- Notfall- und Wiederanlaufplanung (Business Continuity).
- Maximale Wiederherstellungszeit (RTO): 24 Stunden.
- Maximaler Datenverlust (RPO): 24 Stunden.
- Keine eigenen physischen Server, USV- oder Klimasysteme, da Cloud-First-Ansatz.

4. Trennungskontrolle

- Logische Mandantentrennung auf Applikations- und Datenbankebene durch eindeutige Mandanten-IDs und RLS-Policies.
- Trennung von Produktions-, Test- und Entwicklungsumgebungen.
- Keine Verwendung personenbezogener Echtdaten in Testsystemen.
- Keine physische Trennung auf dedizierter Hardware (Cloud-Architektur).

5. Pseudonymisierung und Anonymisierung

- Personenbezogene Daten werden nach Zweckfortfall gelöscht oder anonymisiert.
- Pseudonymisierung personenbezogener Daten, soweit technisch und fachlich sinnvoll.
- Verschlüsselung at-rest in der Datenbank (AES-256).

6. Auftrags- und Subprozessorenkontrolle

- Einsatz von Unterauftragsverarbeitern ausschließlich auf vertraglicher Grundlage.
- Abschluss von Auftragsverarbeitungsverträgen (AVV bzw. DPA) mit allen Subdienstleistern.
- Bewertung von Dienstleistern anhand TOMs, Zertifizierungen und Audit-Berichten.
- Kontrolle über vertraglich vereinbarte Sicherheitsmaßnahmen.

7. Datenschutz- und Sicherheitsmanagement

- Kontakt für datenschutzrechtliche Anfragen: office@rev2.at
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.
- Regelmäßige Schulungs- und Awareness-Maßnahmen zu Datenschutz.
- Vertraulichkeitsverpflichtung sämtlicher Mitarbeiter.
- Dokumentierte Prozesse zur Bearbeitung von Betroffenenrechten.
- Dokumentierter Incident-Response-Prozess für Datenschutz- und Sicherheitsvorfälle.

8. Überprüfung und Weiterentwicklung

- Regelmäßige Überprüfung der TOMs.
- Sicherheitsupdates der eingesetzten Software werden zeitnah eingespielt.
- Anlassbezogene Überprüfung bei Sicherheitsereignissen oder Änderungen der Verarbeitung.
- Kontinuierliche Anpassung an neue Risiken und technische Entwicklungen.

Version 1.0 – Stand 18.05.2026