



KUNDEN- & PARTNERUNTERLAGE · MUSTER

Vereinbarung zur Auftragsverarbeitung

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

Für die Zusammenarbeit mit JK Concepts

Diese Vorlage ordnet JK Concepts als Auftragnehmer und Auftragsverarbeiter ein. Der Auftraggeber ergänzt seine Daten sowie sämtliche projektspezifischen Angaben in den Anlagen. Für eine Unterbeauftragung kann der Auftraggeber selbst Auftragsverarbeiter sein.

Vor Unterzeichnung

Dieses Dokument ist ein Arbeitsmuster und keine Rechtsberatung. Gegenstand, Dauer, Datenarten, betroffene Personen, Weisungen, tatsächliche Sicherheitsmaßnahmen, Unterauftragsverarbeiter und Verarbeitungsorte müssen vollständig und wahrheitsgemäß ergänzt werden. Abweichende Projektbedingungen und besondere Risiken sind rechtlich zu prüfen.

JK Concepts · Julian Kocmut

Grottenhofstraße 9b · 8053 Graz · Österreich

office@jkconcepts.at · www.jkconcepts.at

Dokumentstand: 04. Oktober 2026

Vertragsparteien

Diese Vereinbarung wird zwischen den nachstehend bezeichneten Parteien geschlossen und ergänzt den in Anlage 1 bezeichneten Hauptvertrag beziehungsweise Auftrag.

AUFTRAGGEBER	AUFTRAGNEHMER
Firma / Name: _____ Anschrift: _____ _____ Kontakt / E-Mail: _____ Rolle: ☐ Verantwortlicher ☐ Auftragsverarbeiter bei Unterbeauftragung	JK Concepts, Julian Kocmut Webdesign & Webentwicklung Grottenhofstraße 9b 8053 Graz · Österreich office@jkconcepts.at Rolle: Auftragsverarbeiter bzw. Unterauftragsverarbeiter

Rollen vorab prüfen

Eine Vereinbarung nach Art. 28 DSGVO ist nur erforderlich, wenn personenbezogene Daten im Auftrag verarbeitet werden. Bestimmt eine Partei selbst über Zwecke und wesentliche Mittel der Verarbeitung, kann stattdessen eine eigene oder gemeinsame Verantwortlichkeit vorliegen.

1. Gegenstand und Rangfolge

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Zusammenhang mit den in Anlage 1 beschriebenen Leistungen. Anlage 1 legt insbesondere Gegenstand und Dauer, Art und Zweck der Verarbeitung, Datenarten, Kategorien betroffener Personen sowie die Rechte und Pflichten des Auftraggebers fest.

1.2 Soweit ein Angebot, Werkvertrag, Wartungs-, Hosting-, Support- oder sonstiger Leistungsvertrag besteht (zusammen „Hauptvertrag“), ergänzt diese Vereinbarung den Hauptvertrag. Bei Widersprüchen gehen zwingendes Datenschutzrecht und anschließend diese Vereinbarung den Regelungen des Hauptvertrags vor, soweit der Widerspruch die Auftragsverarbeitung betrifft.

1.3 Die Anlagen sind Bestandteil dieser Vereinbarung. Projektspezifische dokumentierte Weisungen und Ergänzungen bedürfen zumindest der Textform.

2. Weisungsgebundene Verarbeitung

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und nur im vereinbarten Umfang. Dies gilt auch für Übermittlungen an ein Drittland oder eine internationale Organisation.

2.2 Ist der Auftragnehmer nach Unionsrecht oder dem Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, informiert er den Auftraggeber vor der Verarbeitung über diese rechtliche Anforderung, soweit das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses verbietet.

2.3 Weisungen können in Textform an die in Anlage 1 benannten Kontaktstellen erteilt werden. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Der Auftragnehmer dokumentiert die Weisungen in angemessener Weise.

2.4 Hält der Auftragnehmer eine Weisung für datenschutzwidrig, informiert er den Auftraggeber unverzüglich. Er darf die Ausführung der betroffenen Weisung aussetzen, bis der Auftraggeber sie bestätigt oder ändert.

3. Vertraulichkeit und eingesetzte Personen

3.1 Der Auftragnehmer stellt sicher, dass Personen mit Zugang zu den Daten diese nur nach Weisung verarbeiten, sofern sie nicht gesetzlich zu einer Verarbeitung verpflichtet sind.

3.2 Der Auftragnehmer verpflichtet alle zur Verarbeitung befugten Personen vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit oder stellt sicher, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung gilt auch nach Ende ihrer Tätigkeit fort.

3.3 Zugriffsrechte werden nach dem Erforderlichkeitsprinzip vergeben, regelmäßig überprüft und bei Wegfall der Erforderlichkeit entzogen.

4. Sicherheit der Verarbeitung

4.1 Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Risiken geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO.

4.2 Die für den Auftrag maßgeblichen Maßnahmen werden in Anlage 2 konkretisiert. Beschrieben werden nur tatsächlich umgesetzte Maßnahmen. Der Auftragnehmer darf Maßnahmen weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

4.3 Der Auftragnehmer unterstützt den Auftraggeber mit den ihm verfügbaren Informationen bei der Prüfung, ob das Schutzniveau dem Risiko angemessen ist.

5. Rechte betroffener Personen

5.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung durch geeignete Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO fristgerecht zu bearbeiten.

5.2 Geht ein Antrag unmittelbar beim Auftragnehmer ein, leitet er ihn unverzüglich an den Auftraggeber weiter. Er beantwortet den Antrag nur auf Weisung oder mit Ermächtigung des Auftraggebers.

5.3 Der Auftraggeber bleibt dafür verantwortlich, die Zulässigkeit eines Antrags zu prüfen und gegenüber der betroffenen Person zu entscheiden.

6. Unterstützung und Datenschutzverletzungen

6.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Risikobewertungen, Meldungen an Aufsichtsbehörden, Benachrichtigungen betroffener Personen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

6.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist. Die Mitteilung enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten und Personen, wahrscheinliche Folgen, bereits ergriffene oder vorgeschlagene Maßnahmen sowie eine Kontaktstelle. Fehlende Informationen werden ohne unangemessene Verzögerung nachgereicht.

6.3 Der Auftragnehmer trifft angemessene Maßnahmen zur Eindämmung, Beweissicherung und Behebung des Vorfalls. Meldungen an Behörden oder betroffene Personen erfolgen durch den Auftraggeber, soweit der Auftragnehmer nicht gesetzlich selbst dazu verpflichtet ist.

7. Nachweise, Kontrollen und Verzeichnis

7.1 Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind. Er führt, soweit gesetzlich erforderlich, ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

7.2 Der Auftraggeber ist berechtigt, die Einhaltung dieser Vereinbarung selbst oder durch zur Vertraulichkeit verpflichtete Prüfer zu kontrollieren. Prüfungen sind in der Regel mit angemessener Vorlaufzeit anzukündigen, während üblicher Geschäftszeiten durchzuführen und auf das erforderliche Maß zu beschränken. Bei konkretem Verdacht auf einen erheblichen Verstoß oder bei einem Sicherheitsvorfall kann die Ankündigungsfrist angemessen verkürzt werden.

7.3 Gleichwertige aktuelle Prüfberichte, Zertifizierungen oder andere geeignete Nachweise können berücksichtigt werden. Betriebs- und Geschäftsgeheimnisse sowie Rechte anderer Kunden sind zu schützen. Gesetzliche Kontrollbefugnisse bleiben unberührt.

8. Unterauftragsverarbeiter

8.1 Der Auftragnehmer darf Unterauftragsverarbeiter nur nach vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Auftraggebers einsetzen. Die gewählte Genehmigungsform und eine allfällige Informationsfrist werden in Anlage 3 festgelegt. Bei allgemeiner Genehmigung informiert der Auftragnehmer den Auftraggeber innerhalb der vereinbarten Frist über beabsichtigte Änderungen, damit der Auftraggeber aus sachlich berechtigten Datenschutzgründen widersprechen kann.

8.2 Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich im Wesentlichen zu denselben Datenschutzpflichten. Er bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.

8.3 Anlage 3 ist aktuell zu halten. Reine Nebenleistungen ohne Zugriff auf personenbezogene Daten sind keine Unterauftragsverarbeitung.

9. Verarbeitungsorte und internationale Übermittlungen

9.1 Die vereinbarten Verarbeitungsorte werden in Anlage 1 und Anlage 3 dokumentiert. Änderungen bedürfen einer dokumentierten Weisung oder Genehmigung des Auftraggebers.

9.2 Eine Übermittlung in ein Drittland oder an eine internationale Organisation erfolgt nur, wenn die Voraussetzungen des Kapitels V DSGVO erfüllt sind. Erforderliche Garantien, insbesondere Angemessenheitsbeschlüsse oder geeignete Standarddatenschutzklauseln einschließlich ergänzender Maßnahmen, werden dokumentiert.

9.3 Diese Vorlage ersetzt keine Standardvertragsklauseln für internationale Datenübermittlungen.

10. Rückgabe, Löschung und Vertragsende

10.1 Nach Abschluss der vertraglichen Leistungen löscht oder gibt der Auftragnehmer nach dokumentierter Wahl des Auftraggebers alle im Auftrag verarbeiteten personenbezogenen Daten und vorhandenen Kopien zurück, sofern keine gesetzliche Aufbewahrungspflicht besteht. Die Wahl und die Frist werden in Anlage 1 festgelegt.

10.2 Soweit Daten in Sicherungskopien nicht sofort selektiv gelöscht werden können, werden sie bis zur planmäßigen Überschreibung gesperrt und nicht weiter verarbeitet, sofern nicht eine Wiederherstellung zur Gefahrenabwehr erforderlich ist.

10.3 Bei einer Rückgabe stellt der Auftragnehmer die Daten im vereinbarten oder in einem gängigen, maschinenlesbaren Format bereit, soweit dies technisch möglich und im Leistungsumfang vorgesehen ist.

10.4 Vertraulichkeits-, Nachweis- und Haftungspflichten, die ihrer Natur nach fortgelten, bleiben nach Vertragsende bestehen.

11. Pflichten und Rechte des Auftraggebers

11.1 Der Auftraggeber bestimmt Zwecke und wesentliche Mittel der Verarbeitung, stellt die Rechtmäßigkeit der Verarbeitung sicher und erteilt eindeutige, rechtmäßige und dokumentierte Weisungen.

11.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich über Fehler, Unregelmäßigkeiten oder besondere Risiken, die er bei der Prüfung der Auftragsergebnisse feststellt. Er benennt erreichbare Kontaktstellen für Weisungen und Sicherheitsvorfälle.

11.3 Der Auftraggeber ist berechtigt, Weisungen zu erteilen, Nachweise anzufordern, Kontrollen nach Punkt 7 durchzuführen und die Rückgabe oder Löschung nach Punkt 10 zu verlangen.

12. Dauer, Beendigung und sonstige Bestimmungen

12.1 Beginn, Laufzeit und Kündigung ergeben sich aus Anlage 1 und dem Hauptvertrag. Das Recht zur außerordentlichen Beendigung aus wichtigem Grund bleibt unberührt.

12.2 Verstößt der Auftragnehmer erheblich oder wiederholt gegen diese Vereinbarung oder die DSGVO, kann der Auftraggeber Weisungen zur Abhilfe erteilen, die Verarbeitung aussetzen und – wenn eine Abhilfe nicht möglich ist oder nicht fristgerecht erfolgt – den betroffenen Auftrag beenden.

12.3 Änderungen und Ergänzungen dieser Vereinbarung bedürfen zumindest der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Individuelle Abreden bleiben unberührt.

12.4 Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Es gilt österreichisches Recht, soweit eine Rechtswahl zulässig ist und der Hauptvertrag nichts Abweichendes vorsieht.

Unterzeichnung

Die Parteien bestätigen, dass Anlage 1 bis Anlage 3 vollständig ausgefüllt, geprüft und Bestandteil dieser Vereinbarung sind.

Ort, Datum	Ort, Datum
------------	------------

Auftraggeber / zeichnungsberechtigte Person	JK Concepts / Julian Kocmut
---	-----------------------------

Anlage 1 · Beschreibung der Verarbeitung

Diese Anlage enthält die nach Art. 28 Abs. 3 DSGVO erforderlichen projektspezifischen Angaben. Nicht Zutreffendes streichen; fehlende Angaben ergänzen.

Hauptvertrag / Angebot / Projekt und Datum
Bezeichnung und eindeutige Referenz

Leistungsbereich

- | | |
|---|---|
| ☐ Website- oder Shop-Entwicklung | ☐ Wartung und technischer Betrieb |
| ☐ Hosting / Serveradministration | ☐ Support und Fehleranalyse |
| ☐ Migration / Import / Export | ☐ Analyse, Monitoring oder Backups |
| ☐ E-Mail- oder Systemintegration | ☐ Sonstiges (unten beschreiben) |

Gegenstand, Aufgaben sowie Art und Zweck der Verarbeitung
So konkret wie möglich: Welche Leistung erfordert welche Verarbeitung?

Verarbeitungsvorgänge

- | | |
|--|--|
| ☐ Erheben / Erfassen | ☐ Ordnen / Speichern |
| ☐ Auslesen / Abfragen | ☐ Verändern / Aktualisieren |
| ☐ Übermitteln / Bereitstellen | ☐ Abgleichen / Verknüpfen |
| ☐ Einschränken | ☐ Löschen / Vernichten |

Zusätzliche Beschreibung der Verarbeitungsvorgänge

Anlage 1 · Daten und betroffene Personen

Kategorien personenbezogener Daten

- | | |
|---|---|
| ☐ Stamm- und Kontaktdaten | ☐ Vertrags- und Abrechnungsdaten |
| ☐ Kommunikations- und Supportdaten | ☐ Zugangs- und Berechtigungsdaten |
| ☐ Nutzungs-, Protokoll- und Gerätedaten | ☐ Website-, Formular- und Inhaltsdaten |
| ☐ Bestell-, Buchungs- oder Shopdaten | ☐ Bewerbungs- oder Beschäftigtendaten |
| ☐ Bild-, Audio- oder Videodaten | ☐ Standort- oder Netzwerkdaten |
| ☐ Besondere Kategorien nach Art. 9 DSGVO | ☐ Daten zu Straftaten nach Art. 10 DSGVO |

Datenkategorien konkretisieren

Besondere Kategorien oder Art.-10-Daten ausdrücklich benennen und Schutzbedarf prüfen.

Kategorien betroffener Personen

- | | |
|--|--|
| ☐ Kunden / Auftraggeber | ☐ Interessenten / Websitebesucher |
| ☐ Kontaktpersonen | ☐ Beschäftigte / Bewerber |
| ☐ Lieferanten / Dienstleister | ☐ Nutzer / Mitglieder |
| ☐ Geschäftspartner | ☐ Sonstige (unten beschreiben) |

Betroffenenkategorien konkretisieren

Häufigkeit, Umfang und ungefähre Datenmenge

Einmalig, regelmäßig, anlassbezogen; Größenordnung und Zahl betroffener Personen

Anlage 1 · Laufzeit, Orte und Weisungen

Beginn und Dauer

☐ Einmalige Verarbeitung bis Abschluss der Leistung

☐ Befristet bis: _____

☐ Für die Dauer des Hauptvertrags

☐ Unbefristet; Kündigung nach Hauptvertrag

Abweichende Laufzeit / Kündigungsregel

Aufbewahrung, Rückgabe und Löschfristen

Frist nach Leistungsende; Rückgabeformat; gesetzliche Aufbewahrung; Backup-Zyklus

Verarbeitungsorte

Unternehmensstandorte, Rechenzentren, Cloud-Regionen; zusätzlich Anlage 3 beachten

Drittlandübermittlungen und eingesetzte Garantien

Land, Empfänger, Angemessenheitsbeschluss oder Art.-46-Garantie, ergänzende Maßnahmen

Weisungsberechtigte Personen und Kontakt für Datenschutzvorfälle

Name, Funktion, E-Mail, Telefon

Anlage 2 · Technische und organisatorische Maßnahmen

Dokumentationsregel

Nur tatsächlich umgesetzte und für den Auftrag relevante Maßnahmen ankreuzen. Die Auswahl muss zum Risiko der konkreten Verarbeitung passen. Falls eine gesonderte TOM-Dokumentation besteht, kann sie eindeutig bezeichnet und beigelegt werden.

A. Organisation und Vertraulichkeit

- | | |
|---|---|
| ☐ Vertraulichkeitsverpflichtungen | ☐ Datenschutz- und Sicherheitsschulungen |
| ☐ Rollen- und Berechtigungskonzept | ☐ Need-to-know-Prinzip |
| ☐ Regelmäßige Berechtigungsprüfung | ☐ Vorgaben für Homeoffice / mobiles Arbeiten |
| ☐ Lieferanten- und Unterauftragnehmerprüfung | ☐ Dokumentierte Sicherheitsrichtlinien |

B. Zutritts- und Zugangskontrolle

- | | |
|---|--|
| ☐ Schlüssel- oder Zutrittssystem | ☐ Besucherregelung / Begleitung |
| ☐ Alarm- oder Sicherheitssystem | ☐ Bildschirmsperre |
| ☐ Starke Passwortrichtlinie | ☐ Mehr-Faktor-Authentisierung |
| ☐ Geräte- und Datenträgerverschlüsselung | ☐ Administrationszugänge getrennt |

C. Zugriff und Trennung

- | | |
|---|---|
| ☐ Mandanten- / Projektentrennung | ☐ Rollenbasierte Zugriffe |
| ☐ Protokollierung administrativer Zugriffe | ☐ Regelmäßige Log-Auswertung |
| ☐ Pseudonymisierung, soweit möglich | ☐ Testdaten ohne Echtdaten, soweit möglich |
| ☐ Freigabeprozess für Berechtigungen | ☐ Sichere Datenträgerentsorgung |

Ergänzungen / Verweis auf gesonderte TOM-Dokumentation

Anlage 2 · Integrität, Verfügbarkeit und Verfahren

D. Übertragung und Eingabe

- | | |
|--|--|
| ☐ Transportverschlüsselung | ☐ Verschlüsselte Dateiübermittlung |
| ☐ VPN / abgesicherte Administration | ☐ Protokollierung von Eingaben und Änderungen |
| ☐ Sichere Austauschplattform | ☐ Empfänger- und Berechtigungsprüfung |
| ☐ Schutz von API-Schlüsseln und Secrets | ☐ Integritäts- oder Signaturprüfungen |

E. Verfügbarkeit und Wiederherstellung

- | | |
|---|--|
| ☐ Dokumentierte Backup-Strategie | ☐ Verschlüsselte Backups |
| ☐ Getrennte / externe Sicherung | ☐ Wiederherstellungstests |
| ☐ Firewall und Malware-Schutz | ☐ Patch- und Updateprozess |
| ☐ Monitoring und Alarmierung | ☐ Notfall- und Wiederanlaufplan |

F. Prüfung, Bewertung und Incident Response

- | | |
|---|--|
| ☐ Regelmäßige Sicherheitsüberprüfung | ☐ Schwachstellenmanagement |
| ☐ Dokumentierter Meldeweg | ☐ Incident-Response-Prozess |
| ☐ Ursachenanalyse und Nachverfolgung | ☐ Datenschutzfreundliche Voreinstellungen |
| ☐ Lösch- und Aufbewahrungskonzept | ☐ Änderungs- und Freigabeverfahren |

Auftragsspezifische Maßnahmen, Intervalle und Verantwortlichkeiten

Restrisiken / vereinbarte zusätzliche Maßnahmen

Anlage 3 · Unterauftragsverarbeiter

Der Auftraggeber genehmigt die nachfolgend vollständig aufgeführten Unterauftragsverarbeiter. Bei Drittlandbezug sind die eingesetzte Garantie und gegebenenfalls ergänzende Maßnahmen anzugeben.

☐ Vorherige gesonderte Genehmigung

☐ Allgemeine schriftliche Genehmigung mit Widerspruchsrecht

Unternehmen / Kontakt	Leistung	Verarbeitungsort	Garantie bei Drittland

Informationsfrist bei allgemeiner Genehmigung

Frist vor Einsatz eines neuen oder ersetzten Unterauftragsverarbeiters

Aktualisierung

Änderungen dieser Liste müssen dem Auftraggeber entsprechend Punkt 8 vor Einsatz des neuen oder ersetzten Unterauftragsverarbeiters mitgeteilt werden. Die jeweils freigegebene Fassung ist gemeinsam mit der Vereinbarung aufzubewahren.

Hinweise zur Verwendung und Quelle

Einsatzbereich. Die bereitgestellte Ausgangsvorlage ist auf Auftragsverarbeitungen in Österreich zugeschnitten. Für Auftragsverarbeitungen innerhalb der EU, des EWR oder in Staaten mit angemessenem Datenschutzniveau empfiehlt die aktuelle DSGVO4KMU-Information die Standardvertragsklauseln der Europäischen Kommission nach Durchführungsbeschluss (EU) 2021/915. Für Übermittlungen in Drittländer können die Standarddatenschutzklauseln nach Durchführungsbeschluss (EU) 2021/914 erforderlich sein.

Inhaltliche Grundlage. DSGVO4KMU / Wirtschaftskammern Österreichs und Österreichische Datenschutzbehörde, „Muster: Vereinbarung für eine Auftragsverarbeitung nach Art. 28 Abs. 3 erster Satz DSGVO“, Dokumentstand August 2026; JK-Redaktion und Neustrukturierung vom 04. Oktober 2026.

Offizielle Quellen. [WKO / DSGVO4KMU-Muster](#) · [DSGVO](#), insbesondere [Art. 28](#) · [Durchführungsbeschluss \(EU\) 2021/915](#)

Keine ungeprüfte Standardlösung

Die Notwendigkeit und Ausgestaltung einer Auftragsverarbeitungsvereinbarung hängt von der tatsächlichen Rollenverteilung und Verarbeitung ab. Diese Unterlage darf erst verwendet oder unterzeichnet werden, nachdem alle offenen Felder projektbezogen ergänzt und rechtlich sowie technisch geprüft wurden.

JK Concepts

Webdesign · Webentwicklung · technischer Betrieb

www.jkconcepts.at · office@jkconcepts.at