# Vereinbarung zur Auftragsverarbeitung einschließlich Anlagen

Entwurf zur Freigabe. Nicht für verbindliche Bestellungen oder freigegebene Kundenauslieferungen verwenden. Offene Felder sind vor Verwendung auszufüllen; rechtliche und kaufmännische Prüfung ist erforderlich.

## 1. Parteien, Gegenstand und Wirksamkeit

Verantwortlicher: Unternehmen, Anschrift und Kontakt [____]. Auftragsverarbeiter: Inceptum Business Solutions GmbH, Erich-Nörrenberg-Straße 7, 58636 Iserlohn, Deutschland, info@inceptumgroup.de. Diese Vereinbarung gilt ausschließlich für die in Anlage A konkret bezeichnete Verarbeitung im Auftrag nach Artikel 28 DSGVO. Sie wird mit wirksamer Vereinbarung durch die Parteien und vollständigen Anlagen A bis C verbindlich. Die bloße Softwarelizenzierung begründet keine Auftragsverarbeitung.

Gegenstand, Art, Zweck, Datenarten, betroffene Personengruppen, Dauer, Verarbeitungsorte und Löschablauf werden in Anlage A festgelegt. Der Verantwortliche bestimmt Zwecke und wesentliche Mittel, stellt eine Rechtsgrundlage sicher, informiert Betroffene und verantwortet die Rechtmäßigkeit seiner Weisungen. Inceptums Pflichten als Auftragsverarbeiter bleiben davon unberührt.

## 2. Weisungen und Vertraulichkeit

Inceptum verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch bei Übermittlungen in Drittländer, sofern keine gesetzliche Pflicht zur Verarbeitung besteht. In diesem Fall informiert Inceptum vorher über die Pflicht, soweit das Gesetz dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Weisungsberechtigte und Empfänger sind in Anlage A benannt. Mündliche Eilweisungen werden unverzüglich dokumentiert.

Hält Inceptum eine Weisung für datenschutzwidrig, informiert es den Verantwortlichen unverzüglich und setzt die betroffene Verarbeitung bis zur Klärung aus, soweit erforderlich. Personen mit Datenzugriff sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht. Zugriff wird nur im erforderlichen Umfang gewährt.

## 3. Sicherheit der Verarbeitung

Inceptum setzt unter Berücksichtigung des Risikos geeignete technische und organisatorische Maßnahmen nach Artikel 32 DSGVO um. Die tatsächlich vereinbarten Maßnahmen und ihre Nachweise sind in Anlage B konkret zu dokumentieren. Schutzbedarf, Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Wiederherstellung und regelmäßige Wirksamkeitsprüfung sind zu berücksichtigen. Änderungen dürfen das vereinbarte Schutzniveau nicht unterschreiten; wesentliche Änderungen werden dokumentiert und mitgeteilt.

Eine leere Maßnahmenliste oder eine Produkt-Sicherheitsbeschreibung gilt nicht als Nachweis umgesetzter betrieblicher Maßnahmen. Vor produktivem Fernzugriff oder Hosting müssen die Maßnahmen geprüft, die Zugriffsmittel festgelegt und die erforderlichen Freigaben dokumentiert sein.

## 4. Weitere Auftragsverarbeiter und Drittländer

Die in Anlage C namentlich mit Leistung und Verarbeitungsort aufgeführten weiteren Auftragsverarbeiter sind bei Abschluss speziell genehmigt. Jede spätere Hinzuziehung oder Ersetzung bedarf einer vorherigen gesonderten Genehmigung des Verantwortlichen in Textform. Ohne Eintrag besteht keine pauschale Genehmigung. Inceptum verpflichtet diese Unternehmen vertraglich auf dieselben Datenschutzpflichten und bleibt dem Verantwortlichen gegenüber für deren Erfüllung verantwortlich.

Verarbeitungen außerhalb des EWR erfordern zusätzlich zu Weisung und Genehmigung eine zulässige Grundlage nach Kapitel V DSGVO, einschließlich erforderlicher Garantien, Transferprüfung und ergänzender

Maßnahmen. Diese Vereinbarung ist selbst kein Drittland-Transferinstrument. Hosting des Shops bei Mittwald begründet nicht automatisch eine Unterauftragsverarbeitung für sämtliche CRM-Kundendaten.

## 5. Unterstützung und Datenschutzverletzungen

Inceptum unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit geeigneten Maßnahmen bei Betroffenenrechten. Direkt eingehende Anträge werden unverzüglich weitergeleitet und nicht ohne Weisung eigenständig beantwortet, sofern keine gesetzliche Pflicht besteht. Inceptum unterstützt ferner bei Sicherheit, Meldungen an Aufsichtsbehörden, Benachrichtigungen Betroffener, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen im gesetzlichen Umfang unter Berücksichtigung der verfügbaren Informationen.

Eine Verletzung des Schutzes personenbezogener Daten meldet Inceptum dem Verantwortlichen unverzüglich nach Bekanntwerden. Die Meldung enthält, soweit verfügbar, Art und Umfang, betroffene Daten und Personen, Kontaktstelle, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Abhilfemaßnahmen; fehlende Informationen werden schrittweise nachgereicht. Inceptum sichert notwendige Nachweise und unterstützt die Eindämmung. Die gesetzliche Meldefrist des Verantwortlichen ist keine Wartefrist für Inceptum.

## 6. Nachweise und Kontrollen

Inceptum stellt alle zum Nachweis der Pflichten aus Artikel 28 DSGVO erforderlichen Informationen zur Verfügung und ermöglicht Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen beauftragten Prüfer und trägt dazu bei. Kontrollen werden soweit sachgerecht abgestimmt und schützen Geheimnisse anderer Kunden. Dringlichkeit, konkrete Vorfälle und gesetzliche Kontrollrechte dürfen nicht durch Vorankündigungs- oder Kostenregeln vereitelt werden. Kosten zusätzlicher Leistungen werden gegebenenfalls transparent vereinbart; gesetzliche Mitwirkung wird nicht von einer ungeklärten Vergütung abhängig gemacht.

## 7. Ende, Rückgabe und Löschung

Nach Abschluss der Leistungen gibt Inceptum nach Wahl des Verantwortlichen die Daten zurück oder löscht sie einschließlich vorhandener Kopien, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Format, Fristen und Umgang mit Sicherungskopien werden in Anlage A festgelegt. Gesetzlich aufzubewahrende Daten werden gesperrt, nur für diesen Zweck verarbeitet und nach Fristende gelöscht. Die Durchführung wird auf Verlangen nachgewiesen. Vertraulichkeitspflichten gelten fort.

## Anlage A: Konkrete Verarbeitung

Vor Zugriff verbindlich auszufüllen: Hauptvertrag/Leistungsauftrag [____]; genaue Tätigkeit und Zweck [____]; Beginn/Ende [____]; Datenarten [____]; Personengruppen [____]; besondere Kategorien oder Ausschluss solcher Daten [____]; Systeme und Verarbeitungsorte [____]; Weisungsberechtigte und Notfallkontakte beider Parteien [____]; Rückgabeformat und Fristen [____]; Löschung/Backups und Nachweis [____]. Nur tatsächlich benötigte Daten aufnehmen; keine Produktivpasswörter in diese Anlage eintragen.

## Anlage B: Technische und organisatorische Maßnahmen

Für jede Maßnahme sind Umsetzung, Verantwortlicher und Nachweis zu ergänzen: Identitäten/Rollen/MFA [____]; Zugang zu Räumen und Geräten [____]; Transport-/Speicherverschlüsselung und Schlüsselverwaltung [____]; Mandantentrennung [____]; protokollierte, genehmigte Fernwartung [____]; Backup und getestete Wiederherstellung [____]; Patch- und Schwachstellenmanagement [____]; Vertraulichkeit/Schulung [____]; Löschung und Datenträger [____]; Vorfallsprozess [____]; regelmäßige Wirksamkeitsprüfung [____]. Diese Liste enthält Prüfbereiche, keine Behauptung bereits umgesetzter Maßnahmen.

## Anlage C: Weitere Auftragsverarbeiter und Abschluss

Je Unternehmen: rechtlicher Name/Anschrift [____]; konkrete Leistung [____]; Daten/Personengruppen [____]; Verarbeitungs- und Zugriffsorte [____]; Genehmigung [____]; bei Drittlandbezug Transferinstrument und Bewertung [____]. Falls keine weiteren Auftragsverarbeiter eingesetzt werden, ist dies ausdrücklich zu bestätigen. Abschluss: Verantwortlicher, Name/Funktion, Datum und Unterschrift oder nachweisbare elektronische Annahme [____]; Inceptum, Name/Funktion, Datum und Annahme [____].