

AVV Vertrag zur Auftragsbearbeitung

gemäss Art. 9 des Bundesgesetzes über den Datenschutz (DSG) und, soweit anwendbar, Art. 28 DSGVO

AUFTRAGSBEARBEITERIN / AUFTRAGSVERARBEITERIN	AUFTRAGGEBER / VERANTWORTLICHER
Binadoo AG Turmstrasse 28 CH-6312 Steinhausen ZG Schweiz nachfolgend «Binadoo»	[Firma] [Strasse, Nr.] [ISO]-[PLZ] [Ort] [Land] nachfolgend «Auftraggeber»
Anwendungsbereich Diese Vereinbarung gilt nur, soweit Binadoo Personendaten im Auftrag des Auftraggebers bearbeitet. Das Online-Verzeichnis der Unterauftragsbearbeiter und Bearbeitungsstandorte ist unter https://binadoo.com/rechtliches/unterauftragsbearbeiter abrufbar. Direkt vom Auftraggeber beauftragte Plattform- oder Hosting-Anbieter sind insoweit keine Unterauftragsbearbeiter von Binadoo.	

1. Gegenstand, Begriffe und Rangfolge

1.1 Gegenstand. Diese Vereinbarung ergänzt den Vertrag über Beratungs-, Implementierungs-, Entwicklungs-, Migrations-, Hosting-Betreuungs-, Schulungs-, Support- oder sonstige Leistungen rund um Unternehmensprozesse und Odoo (der «Hauptvertrag»). Sie gilt für alle Tätigkeiten, bei denen Binadoo oder ein von Binadoo beigezogener Unterauftragsbearbeiter Personendaten für den Auftraggeber bearbeitet.

1.2 Begriffe. «Auftraggeber-Daten» sind Personendaten beziehungsweise personenbezogene Daten, die Binadoo im Auftrag des Auftraggebers bearbeitet. Die Begriffe «Bearbeitung» und «Verarbeitung» sowie «Auftragsbearbeiterin» und «Auftragsverarbeiterin» werden sinngemäss verwendet. «Online-Verzeichnis» bezeichnet das von Binadoo unter <https://binadoo.com/rechtliches/> veröffentlichte, versionierte Verzeichnis der Unterauftragsbearbeiter und regelmässigen Bearbeitungs- und Zugriffsstandorte. Soweit die DSGVO anwendbar ist, gelten deren Begriffsbestimmungen ergänzend.

1.3 Abgrenzung. Nicht unter diese Vereinbarung fallen Personendaten, die Binadoo als eigenständig Verantwortliche insbesondere zur Vertragsanbahnung, Vertragsverwaltung, Rechnungsstellung, Erfüllung eigener gesetzlicher Pflichten oder Sicherung der eigenen Geschäftssysteme bearbeitet. Vollständig anonymisierte Informationen sind keine Auftraggeber-Daten.

1.4 Rangfolge. Art, Zweck, Dauer, Datenkategorien und betroffene Personen ergeben sich aus dem Hauptvertrag und Anlage 1. Bei Widersprüchen geht diese Vereinbarung für datenschutzrechtliche Fragen dem Hauptvertrag, den AGB und der Vertraulichkeitsvereinbarung vor. Im Übrigen gelten diese Vereinbarungen nebeneinander.

2. Verantwortlichkeiten und Weisungen

2.1 Verantwortung des Auftraggebers. Der Auftraggeber ist für die Rechtmässigkeit der Bearbeitung, die Rechtsgrundlagen, Informationspflichten, Datenminimierung, Richtigkeit, Aufbewahrungsfristen, Betroffenenrechte sowie den Inhalt seiner Weisungen verantwortlich. Er stellt sicher, dass er Auftraggeber-Daten Binadoo und den genehmigten Unterauftragsbearbeitern rechtmässig zugänglich machen darf.

2.2 Dokumentierte Weisungen. Binadoo bearbeitet Auftraggeber-Daten ausschliesslich auf dokumentierte Weisung des Auftraggebers und nur für die vereinbarten Zwecke. Der Hauptvertrag, diese Vereinbarung, freigegebene Projektunterlagen, Tickets, E-Mails und Weisungen autorisierter Kontaktpersonen gelten als dokumentierte Weisungen. Dies umfasst auch Weisungen zu Bekanntgaben ins Ausland.

2.3 Gesetzliche Pflichten und unzulässige Weisungen. Ist Binadoo aufgrund zwingenden Rechts zu einer weiteren Bearbeitung verpflichtet, informiert sie den Auftraggeber vorgängig, soweit dies rechtlich zulässig ist. Hält Binadoo eine Weisung für datenschutzwidrig, informiert sie den Auftraggeber unverzüglich und darf deren Ausführung bis zu einer rechtmässigen Klärung aussetzen. Bleibt eine rechtmässige Leistungserbringung unmöglich, kann die betroffene Leistung aus wichtigem Grund beendet werden.

2.4 Besondere Risiken. Der Auftraggeber informiert Binadoo vorab, wenn besonders schützenswerte Personendaten, besondere Kategorien personenbezogener Daten, Straftaten, Daten von Kindern, umfangreiche Überwachungsdaten, Hochrisiko-Profilung oder automatisierte Einzelentscheidungen bearbeitet werden sollen. Nicht in Anlage 1 bezeichnete Hochrisikobearbeitungen bedürfen vor Beginn einer Ergänzung der Weisung und, soweit erforderlich, der Schutzmassnahmen.

3. Vertraulichkeit und befugte Personen

3.1 Zugriff. Binadoo gewährt Auftraggeber-Daten nur Personen Zugriff, die diese zur Vertragserfüllung benötigen. Zugriffe werden nach dem Need-to-know- und Least-Privilege-Prinzip vergeben und nach Wegfall des Bedarfs entzogen.

3.2 Verpflichtung. Binadoo stellt sicher, dass befugte Personen vor dem Zugriff angemessen auf Vertraulichkeit verpflichtet oder einer gesetzlichen Verschwiegenheitspflicht unterstellt und zu Datenschutz sowie Informationssicherheit instruiert sind. Die Pflichten gelten nach Ende ihres Einsatzes fort.

4. Datensicherheit und Verantwortungsbereiche

4.1 Schutzmassnahmen. Binadoo trifft die in Anlage 2 beschriebenen, dem Risiko angemessenen technischen und organisatorischen Massnahmen. Sie berücksichtigt den Stand der Technik, Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Bearbeitung. Binadoo darf Massnahmen weiterentwickeln, sofern das vereinbarte Schutzniveau insgesamt nicht wesentlich unterschritten wird.

4.2 Verantwortungsbereiche. Die Massnahmen von Binadoo gelten für ihren Einflussbereich. Der Auftraggeber verantwortet insbesondere Dateninhalte, Benutzer- und Rollenmodelle, Freigaben, eigene Endgeräte und Netze, kundenseitige Integrationen sowie On-Premise-Infrastruktur und Datensicherungen, soweit diese nicht ausdrücklich von Binadoo geschuldet sind. Für Test- und Entwicklungsumgebungen sind nach Möglichkeit anonymisierte oder pseudonymisierte Daten zu verwenden.

4.3 Plattformanbieter. Werden Plattform-, Cloud- oder Hosting-Leistungen eingesetzt, gelten deren technische und organisatorische Massnahmen für den jeweiligen Verantwortungsbereich ergänzend. Verfügbarkeiten, Sicherungszyklen, Speicherorte und Wiederherstellungswerte richten sich nach dem Hauptvertrag und den Bedingungen des jeweiligen Anbieters.

5. Unterauftragsbearbeiter

5.1 Allgemeine Genehmigung und Online-Verzeichnis. Der Auftraggeber genehmigt den Beizug der in Anlage 3 und im Online-Verzeichnis aufgeführten Unterauftragsbearbeiter. Die bei Vertragsabschluss veröffentlichte Version des Online-Verzeichnisses ist Bestandteil dieser Vereinbarung. Das Verzeichnis nennt mindestens Identität und Sitz des direkten Unterauftragsbearbeiters, die übertragene Leistung, die regelmässigen Bearbeitungs- und Zugriffsstandorte sowie die Kategorie der eingesetzten Transfergarantie. Die bei Vertragsabschluss massgebende Erstversion wird in Anlage 3 mit Versions- oder Veröffentlichungsdatum bezeichnet.

5.2 Änderungen und Vorabinformation. Binadoo informiert den Auftraggeber mindestens 14 Kalendertage vor dem geplanten erstmaligen Einsatz eines neuen oder ersetzten direkten Unterauftragsbearbeiters sowie vor dem erstmaligen regelmässigen Zugriff aus einem zusätzlichen Staat. Die Mitteilung erfolgt in Textform an die in Anlage 1 bezeichnete Datenschutzkontaktstelle oder über einen vereinbarten Benachrichtigungsdienst. Die Entfernung eines Anbieters oder Standorts sowie rein redaktionelle Änderungen können ohne Vorlaufzeit im Online-Verzeichnis nachgeführt werden.

5.3 Einspruch. Der Auftraggeber kann innerhalb der Mitteilungsfrist aus nachvollziehbaren datenschutzrechtlichen Gründen Einspruch erheben. Die Parteien prüfen eine zumutbare Alternative. Ist keine solche verfügbar, kann jede Partei die betroffene Leistung auf den Zeitpunkt des geplanten Einsatzes oder den nächstmöglichen Termin beenden. Erfolgt kein fristgerechter Einspruch, gilt die angekündigte Änderung als genehmigt.

5.4 Pflichten, weitere Unterbeauftragung und Verantwortung. Binadoo verpflichtet direkte Unterauftragsbearbeiter vertraglich zu einem im Wesentlichen gleichwertigen Datenschutz- und Sicherheitsniveau und bleibt gegenüber dem Auftraggeber für die Erfüllung der übertragenen Pflichten verantwortlich. Ein direkter Unterauftragsbearbeiter darf weitere eigenständige Unterauftragsbearbeiter nur mit vorgängiger Genehmigung von Binadoo und unter Einhaltung einer gleichwertigen Pflichtenkette beziehen.

5.5 Befugte Personen und internationale Teams. Mitarbeitende sowie natürliche Personen, die unter der unmittelbaren Weisungs-, Organisations- und Vertraulichkeitsbindung von Binadoo oder eines genehmigten Unterauftragsbearbeiters handeln, gelten als befugte Personen und werden nicht einzeln öffentlich aufgeführt. Voraussetzung ist, dass sie Auftraggeber-Daten weder für eigene Zwecke bearbeiten noch weitere Personen beziehen und ausschliesslich aus im Online-Verzeichnis genannten Staaten zugreifen. Handelt eine Person oder ihre eigene Gesellschaft als eigenständige Leistungserbringerin, gilt sie als weitere Unterauftragsbearbeiterin und unterliegt Ziffern 5.1 bis 5.4.

5.6 Direkt beauftragte Anbieter. Vom Auftraggeber direkt beauftragte Software-, Plattform- oder Hosting-Anbieter sind keine Unterauftragsbearbeiter von Binadoo. Der Auftraggeber ist für deren Auswahl und vertragliche Datenschutzgrundlage verantwortlich; Binadoo unterstützt die technische Einbindung im vereinbarten Umfang.

6. Bekanntgabe ins Ausland

6.1 Bearbeitungs- und Zugriffsstandorte. Eine Bearbeitung oder ein Remote-Zugriff ausserhalb der Schweiz beziehungsweise, soweit die DSGVO anwendbar ist, ausserhalb des EU-/EWR-Raums erfolgt nur nach Massgabe des anwendbaren Datenschutzrechts. Ein Zugriff aus einem Staat gilt für diese Vereinbarung als Bearbeitung an diesem Standort. Regelmässige Zugriffe aus einem nicht im Online-Verzeichnis aufgeführten Staat sind untersagt, bis das Verfahren gemäss Ziffer 5.2 abgeschlossen ist. Die Aufnahme eines Staates in das Online-Verzeichnis dient zugleich der Transparenz und der internen Zugriffsfreigabe; sie entscheidet nicht vorweg, ob ein konkreter Zugriff rechtlich als Bekanntgabe beziehungsweise Übermittlung an eine separate Empfängerin einzustufen ist.

6.2 Angemessenheit und geeignete Garantien. Liegt für den betreffenden Staat, das Gebiet, den Sektor oder die konkrete Empfängerin ein anerkannter Angemessenheitsentscheid vor, darf die Bearbeitung innerhalb dessen Geltungsbereich erfolgen. Andernfalls stellt Binadoo beziehungsweise der betroffene Unterauftragsbearbeiter vor einer Bekanntgabe an eine separate Empfängerin eine zulässige Garantie sicher, insbesondere anerkannte Standardvertragsklauseln mit den für das Schweizer Recht erforderlichen Anpassungen oder eine andere gesetzlich anerkannte Grundlage. Soweit erforderlich, werden eine Transfer-Risikoprüfung und ergänzende technische und organisatorische Massnahmen dokumentiert.

6.3 Transparenz und Nachweise. Das Online-Verzeichnis weist die regelmässigen Staaten und die jeweilige Kategorie der Schutzgrundlage aus. Binadoo stellt dem Auftraggeber auf begründete Anfrage angemessene Informationen zu den eingesetzten Transfermechanismen zur Verfügung. Vertragsunterlagen, Risikoanalysen und Sicherheitsnachweise dürfen zum Schutz von Rechten Dritter, Geschäftsgeheimnissen und Sicherheitsinteressen angemessen geschwärzt oder durch geeignete Bestätigungen ersetzt werden.

7. Unterstützung des Auftraggebers

7.1 Betroffenenrechte. Erhält Binadoo ein Begehren einer betroffenen Person zu Auftraggeber-Daten, leitet sie es unverzüglich an den Auftraggeber weiter und beantwortet es nicht selbst, sofern sie hierzu nicht angewiesen oder gesetzlich verpflichtet ist. Unter Berücksichtigung der Art der Bearbeitung unterstützt Binadoo den Auftraggeber mit geeigneten technischen und organisatorischen Massnahmen bei der Erfüllung von Betroffenenrechten.

7.2 Weitere Pflichten. Binadoo unterstützt den Auftraggeber unter Berücksichtigung der verfügbaren Informationen in angemessenem Umfang bei Datensicherheit, Verletzungen der Datensicherheit, Datenschutz-Folgenabschätzungen, vorgängigen Konsultationen und Anfragen zuständiger Behörden. Der Auftraggeber bleibt für seine rechtliche Beurteilung, Entscheide und Meldungen verantwortlich.

7.3 Vergütung. Unterstützung, die über die vertraglich geschuldeten Standardleistungen hinausgeht, wird nach Aufwand zu den vereinbarten Ansätzen vergütet, sofern sie nicht durch eine von Binadoo zu vertretende Vertragsverletzung verursacht wurde.

8. Verletzungen der Datensicherheit

8.1 Meldung. Binadoo meldet dem Auftraggeber unverzüglich, nachdem sie von einer Verletzung der Datensicherheit im Zusammenhang mit Auftraggeber-Daten Kenntnis erlangt hat. Die Erstmeldung enthält die zu diesem Zeitpunkt verfügbaren Angaben zu Art und Umfang, betroffenen Daten und Personen, wahrscheinlichen Folgen, Kontaktstelle sowie ergriffenen oder vorgeschlagenen Massnahmen. Fehlende Angaben werden ohne unangemessene Verzögerung nachgereicht.

8.2 Massnahmen und Dokumentation. Binadoo trifft angemessene Massnahmen zur Eindämmung, Untersuchung und Behebung, sichert erforderliche Nachweise und dokumentiert den Vorfall im gesetzlich erforderlichen Umfang. Die Parteien koordinieren ihre Kommunikation. Meldungen an Behörden und betroffene Personen obliegen dem Auftraggeber, soweit Binadoo nicht gesetzlich selbst verpflichtet ist oder ausdrücklich beauftragt wird.

9. Nachweise und Prüfungen

9.1 Nachweise. Binadoo stellt auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung erforderlich sind. Einschlägige Zertifikate, Auditberichte, Anbieter-Nachweise, Sicherheitsdokumentationen und standardisierte Fragebogen können als Nachweis berücksichtigt werden.

9.2 Prüfungen. Der Auftraggeber darf die Einhaltung grundsätzlich einmal pro Kalenderjahr sowie zusätzlich bei konkreten Anzeichen einer wesentlichen Nichteinhaltung prüfen oder durch eine unabhängige, nicht konkurrierende und zur Vertraulichkeit verpflichtete Fachperson prüfen lassen. Prüfungen sind mindestens 20 Arbeitstage vorher anzukündigen, während üblicher Geschäftszeiten durchzuführen und auf den erforderlichen Umfang zu beschränken.

Daten anderer Kunden, Quellcode, Schwachstellendetails und Geschäftsgeheimnisse dürfen nicht offengelegt werden, soweit ein gleichwertiger Nachweis möglich ist.

9.3 Kosten und Behörden. Der Auftraggeber trägt seine und die durch eine Prüfung verursachten angemessenen Aufwände von Binadoo. Ergibt die Prüfung eine wesentliche, von Binadoo zu vertretende Nichteinhaltung, trägt Binadoo die angemessenen Kosten der Nachprüfung. Zwingende Prüf- und Auskunftsrechte von Aufsichtsbehörden bleiben vorbehalten.

10. Rückgabe und Löschung

10.1 Vertragsende. Nach Ende der auftragsbezogenen Leistungen gibt Binadoo die Auftraggeber-Daten nach Wahl des Auftraggebers in einem vereinbarten oder üblichen maschinenlesbaren Format zurück oder löscht sie, soweit keine gesetzliche Aufbewahrungspflicht besteht. Der Auftraggeber sorgt rechtzeitig für Export und Übernahme; weitergehende Migrations- oder Aufbereitungsleistungen werden nach Aufwand vergütet.

10.2 Sicherungskopien und Nachweis. Technische Sicherungskopien, Protokolle oder nicht selektiv löschbare Archive dürfen bis zu ihrer planmässigen Überschreibung aufbewahrt werden. Sie werden nicht operativ verwendet, bleiben geschützt und unterliegen weiterhin dieser Vereinbarung. Binadoo bestätigt die Löschung auf angemessene Anfrage in Textform.

11. Dauer, Haftung und Schlussbestimmungen

11.1 Dauer. Diese Vereinbarung tritt mit Unterzeichnung oder mit Beginn der ersten Auftragsbearbeitung in Kraft. Sie kann nicht isoliert gekündigt werden, solange Binadoo Auftraggeber-Daten bearbeitet. Nach Ende des Hauptvertrags gilt sie bis zur vollständigen Rückgabe oder Löschung fort.

11.2 Haftung. Haftung und interner Ausgleich zwischen den Parteien richten sich nach dem Hauptvertrag und den wirksam einbezogenen AGB. Zwingende gesetzliche Ansprüche, Befugnisse von Aufsichtsbehörden und Rechte betroffener Personen werden dadurch nicht eingeschränkt.

11.3 Textform, Online-Verzeichnis und Änderungen. Änderungen und Ergänzungen bedürfen der Textform; E-Mail, elektronische Signatur und Austausch unterzeichneter PDF-Kopien genügen. Aktualisierungen des Online-Verzeichnisses nach dem Verfahren gemäss Ziffer 5 bedürfen keiner erneuten Unterzeichnung. Binadoo archiviert die veröffentlichten Versionen so, dass der zu einem bestimmten Zeitpunkt genehmigte Stand nachvollzogen werden kann. Sonstige Aktualisierungen der Anlagen können in Textform vereinbart werden, sofern das Schutzniveau nicht wesentlich reduziert wird.

11.4 Recht und Gerichtsstand. Diese Vereinbarung unterliegt materiellem Schweizer Recht unter Ausschluss seiner kollisionsrechtlichen Bestimmungen. Ausschliesslicher Gerichtsstand ist Zug, Schweiz. Zwingende gesetzliche Gerichtsstände bleiben vorbehalten.

Unterschriften

Binadoo AG	[Firma Auftraggeber]
Ort: _____	Ort: _____
Datum: _____	Datum: _____
Name: _____	Name: _____
Funktion: _____	Funktion: _____
Unterschrift: _____	Unterschrift: _____

Anlage 1 – Beschreibung der Auftragsbearbeitung

Diese Anlage ist vor Unterzeichnung beziehungsweise vor Beginn einer neuen Bearbeitung zu vervollständigen. Massgeblich sind nur die tatsächlich vereinbarten und angekreuzten Leistungen und Datenkategorien.

Angabe	Vereinbarung
Hauptvertrag / Projekt	[Angebot, Auftragsbestätigung oder Projektbezeichnung / Datum]
Leistungen	☐ Odoo Online / Odoo.sh Hosting-Betreuung ☐ Konfiguration, Entwicklung und Schnittstellen ☐ Datenmigration und Datenbereinigung ☐ Support, Wartung und Upgrades ☐ Schulung mit Zugriff auf Echt- oder Testdaten ☐ Externe Entwicklungs- oder Supportleistungen über genehmigte Unterauftragsbearbeiter ☐ Weitere: _____
Art der Bearbeitung	Zugriff, Erheben, Erfassen, Ordnen, Speichern, Anpassen, Abfragen, Übermitteln, Abgleichen, Migrieren, Testen, Sichern, Exportieren und Löschen – jeweils nur soweit für die vereinbarte Leistung erforderlich.
Zwecke	Analyse, Umsetzung, Betrieb, Fehlerbehebung, Support, Migration, Integration, Schulung und Weiterentwicklung der vereinbarten Odoo-Lösung.
Dauer	Während der Laufzeit der betroffenen Leistungen sowie bis zur Rückgabe oder Löschung nach Ziffer 10.
Hosting- / Betriebsmodell	☐ Odoo Online, direkt durch Auftraggeber beauftragt ☐ Odoo.sh, direkt durch Auftraggeber beauftragt ☐ Hosting-Anbieter durch Binadoo beauftragt ☐ Hosting-Anbieter direkt durch Auftraggeber beauftragt ☐ On-Premise beim Auftraggeber ☐ Sonstiges: _____
Bearbeitungsorte	Schweiz, EU/EWR und die jeweils genehmigten Staaten gemäss Anlage 3 und Online-Verzeichnis. Regelmässige Zugriffe aus weiteren Staaten sind vor Abschluss des Verfahrens nach Ziffer 5.2 unzulässig. Bei direkt beauftragten Anbietern gelten ergänzend deren Vertragsunterlagen.

1. Datenkategorien

Kategorie	Beispiele / Präzisierung
☐ Identitäts- und Stammdaten	Name, Firma, Funktion, Kundennummer, Geburtsdatum, Identifikatoren
☐ Kontakt- und Kommunikationsdaten	Adresse, Telefon, E-Mail, Nachrichten, Termine, Korrespondenz
☐ Benutzer-, Geräte- und Protokolldaten	Benutzerkonto, Rollen, IP-Adresse, Geräteinformationen, Login- und Systemprotokolle
☐ CRM-, Verkaufs- und Einkaufsdaten	Leads, Offerten, Aufträge, Verträge, Kaufhistorie, Lieferanten- und Partnerdaten
☐ Finanz-, Zahlungs- und Buchhaltungsdaten	Rechnungen, Bank- und Zahlungsdaten, Buchungen, Kostenstellen, Mahnungen
☐ Personal-, Lohn- und Zeitdaten	Arbeitsverhältnis, Lohn, Arbeitszeit, Abwesenheiten, Leistungs- und Spesendaten
☐ Bewerbungs- und Ausbildungsdaten	Lebenslauf, Qualifikationen, Bewerbungsunterlagen, Lern- und Schulungsdaten
☐ Inhalts-, Dokument- und Dateidaten	Dokumente, Anhänge, Notizen, Bilder, Signaturen, individuell gespeicherte Inhalte
☐ Standort- und Bewegungsdaten	Arbeits-, Liefer-, Einsatz- oder Gerätepositionen, soweit eingesetzt
☐ Weitere Daten	_____

2. Besonders schützenswerte Daten und Hochrisikobearbeitungen

Auswahl	Präzisierung
☐ Keine vorgesehen	Es sollen keine besonders schützenswerten oder besonderen Kategorien bearbeitet werden.
☐ Gesundheits-, Abwesenheits- oder Sozialdaten	Diagnosen, Arztzeugnisse, Versicherungs- oder Sozialhilfedaten
☐ Religiöse, weltanschauliche, politische oder gewerkschaftliche Angaben	Nur soweit für den vereinbarten Zweck erforderlich
☐ Genetische oder biometrische Daten	Nur zur eindeutigen Identifizierung, soweit ausdrücklich vereinbart
☐ Daten zu strafrechtlichen oder administrativen Sanktionen und Verfahren	Strafregister-, Verfahrens- oder Sanktionsangaben
☐ Profiling / automatisierte Einzelentscheidungen	Art, Logik und Auswirkungen: _____
☐ Daten von Kindern / besonders vulnerablen Personen	Betroffenengruppe und Zweck: _____
☐ Weitere	_____

3. Kategorien betroffener Personen

Typische Gruppen	Weitere / Einschränkungen
☐ Mitarbeitende, ehemalige Mitarbeitende, Lernende und Praktikanten ☐ Bewerberinnen und Bewerber ☐ Kunden, Interessenten und deren Kontaktpersonen ☐ Lieferanten, Dienstleister und Geschäftspartner ☐ Benutzerinnen und Benutzer des Odoo-Systems ☐ Website-, Portal- oder Veranstaltungsbesucher, soweit im System erfasst ☐ Weitere: _____	[Zu ergänzen, falls einzelne Gruppen ausgeschlossen oder weitere Gruppen erfasst werden] _____ _____

4. Datenschutzkontakte und Weisungen

Partei	Datenschutzkontakt	Weisungsberechtigte / operative Kontakte
Binadoodoo	Binadoodoo AG, Datenschutz info@binadoodoo.com +41 41 510 06 66	Die projektseitig benannten Ansprechpersonen; Änderungen werden in Textform dokumentiert.
Auftraggeber	Name: _____ E-Mail: _____ Telefon: _____	Name(n): _____ E-Mail(s): _____ Funktion(en): _____

Anlage 2 - Technische und organisatorische Massnahmen

Die folgenden Massnahmen gelten für den Einflussbereich von Binadoo. Plattform- und Hosting-Anbieter sowie der Auftraggeber tragen die in dieser Anlage bezeichneten eigenen Verantwortungsbereiche. Die konkrete Ausprägung richtet sich nach Risiko, Projekt und eingesetzten Systemen.

Bereich	Massnahmen
1. Organisation, Rollen und Vertraulichkeit	Definierte Verantwortlichkeiten für Datenschutz und Informationssicherheit; vertragliche Vertraulichkeitsbindung sämtlicher befugter Personen; angemessene Schulung und Sensibilisierung; dokumentierte Prozesse für Eintritt, Rollenwechsel, Austritt, Vorfälle und Löschung.
2. Identitäts- und Zugriffskontrolle	Personalisierte Konten; Need-to-know und Least Privilege; rollen- und projektbezogene Berechtigungen; Mehrfaktor-Authentifizierung für privilegierte und externe Zugänge, soweit technisch unterstützt; zeitnahe Entzug nicht mehr benötigter Rechte.
3. Remote-Arbeit und Länderfreigabe	Remote-Zugriff nur aus genehmigten Staaten und über geschützte Verbindungen; keine Nutzung nicht freigegebener Standorte; vertrauliche Arbeitsumgebung; keine Einsicht durch Haushaltsangehörige oder sonstige Dritte; technische Standort- oder Conditional-Access-Kontrollen, soweit verhältnismässig verfügbar.
4. Endgeräte und Arbeitsplatz	Verwaltete oder gleichwertig kontrollierte Endgeräte mit Festplattenverschlüsselung, Bildschirmsperre, aktuellen Sicherheitsupdates und Schutz vor Schadsoftware; keine Speicherung auf privaten Geräten oder unkontrollierten Datenträgern; sichere Entsorgung.
5. Übermittlung und Geheimnisse	Verschlüsselte Übertragungswege wie TLS/HTTPS, SSH oder VPN; Zugangsdaten über Passwort-Manager oder anderweitig geschützte Kanäle, nicht unverschlüsselt per E-Mail; sichere Verwaltung und Rotation von Passwörtern, Schlüsseln und Tokens.
6. Speicherung, Datenminimierung und Testdaten	Lokale Kopien nur soweit zwingend erforderlich und zeitlich beschränkt; keine dauerhafte lokale Speicherung bei Remote-Personal; Beschränkung von Ticket-, Support- und Entwicklungsdaten; in Test- und Entwicklungsumgebungen nach Möglichkeit anonymisierte oder pseudonymisierte Daten.
7. Trennung, Änderungen und Nachvollziehbarkeit	Logische Trennung von Kunden und Projekten; Trennung von Produktiv-, Test- und Entwicklungsumgebungen, soweit praktikabel; Versionierung von Quellcode; technische Protokollierung und Schutz von Protokolldaten im risikoadäquaten Umfang.
8. Verfügbarkeit und Vorfalldmanagement	Sicherungs-, Redundanz- und Wiederherstellungsmassnahmen gemäss Hostingmodell; definierte Melde- und Eskalationswege; Eindämmung, Untersuchung, Beweissicherung und Nachbereitung von Sicherheitsvorfällen.
9. Löschung und Offboarding	Entzug sämtlicher Zugänge nach Projekt- oder Vertragsende; Löschung temporärer Arbeitskopien; planmässige Überschreibung technischer Backups; dokumentiertes Offboarding von Mitarbeitenden, externen Fachpersonen und Geräten.
10. Lieferanten-, Länder- und Kontrollprozess	Datenschutz- und Sicherheitsanforderungen an Unterauftragsbearbeiter; Prüfung der vertraglichen Einbindung, tatsächlichen Zugriffsstandorte und Transfergrundlagen; keine Aktivierung eines neuen Landes oder eigenständigen Unterauftragsbearbeiters vor Freigabe, Kundeninformation und Ablauf der Einspruchsfrist.

Verantwortungsmatrix

Verantwortlicher Bereich	Primäre Verantwortung
Binadoo	Sicherer Zugriff ihrer Mitarbeitenden und Hilfspersonen; verwaltete Endgeräte; sichere Übermittlung; Projekt- und Berechtigungsorganisation; Schutz temporärer Arbeitskopien; Auswahl und vertragliche Einbindung eigener Unterauftragsbearbeiter.
Plattform- / Hosting-Anbieter	Physische Rechenzentrumssicherheit, Infrastruktur, Plattformbetrieb, technische Mandantentrennung, Plattformprotokolle, Verfügbarkeit, Sicherungen und Wiederherstellung gemäss dessen Vertrag und Sicherheitsdokumentation.
Auftraggeber	Rechtmässigkeit und Inhalt der Daten; Benutzer-, Rollen- und Freigabekonzept; kundenseitige Konten, Endgeräte, Netze und Integrationen; On-Premise-Infrastruktur; fachliche Tests, Aufbewahrung und Datensicherung, soweit nicht ausdrücklich übertragen.

Anlage 3 - Genehmigte Unterauftragsbearbeiter und Bearbeitungsorte

Das aktuelle, versionierte Verzeichnis ist unter <https://binadoodoo.com/rechtliches/> abrufbar. Die nachstehende Tabelle bildet den Stand bei der Erstellung dieser Vorlage ab. Massgebend ist die zuletzt nach Ziffer 5 angekündigte und genehmigte Version. Einzelne Mitarbeitende oder natürliche Personen unter direkter Weisungs- und Organisationshoheit eines aufgeführten Anbieters werden nicht öffentlich namentlich genannt; eigenständige Gesellschaften und weitere Unterauftragsbearbeiter sind dagegen separat aufzuführen. Massgebende Erstversion bei Vertragsabschluss: [Version / Veröffentlichungsdatum].

Unterauftrags- bearbeiter	Leistung	Bearbeitungs- und Zugriffsstandorte	Garantien / Hinweise
Bytebrand Outsourcing AG Turmstrasse 28 CH-6312 Steinhausen ZG CHE-383.370.565	Konfiguration, Entwicklung, Datenmigration, Qualitätssicherung und Support für Odoo-Systeme; projektbezogener Zugriff auf Entwicklungs-, Test- und, soweit erforderlich, Produktivsysteme.	Schweiz. Autorisierte Remote-Zugriffsstandorte, Stand [13.07.2026: Deutschland, Österreich, Polen, Ungarn, Ukraine, Kenia, Aktueller Stand gemäss Online- Verzeichnis.]	AVV und Weisungsbindung mit Binadoodoo; befugte Personen unter direkter Autorität; personalisierte Zugänge, MFA, verschlüsselte Endgeräte und keine dauerhafte lokale Speicherung. Geeignete Garantien nach Art. 16 DSGVO / Kapitel V DSGVO, soweit rechtlich erforderlich.
Google Cloud EMEA Limited 70 Sir John Rogerson's Quay Dublin 2, Irland	Google Workspace für E-Mail, Kalender, Dokumente, Datenaustausch, Chat und Videokonferenzen im Rahmen der Leistungserbringung.	EU/EWR sowie weitere Standorte gemäss Datenregion, Funktionen und aktueller Unterauftragsbearbeiterliste von Google.	Google-Datenverarbeitungsbedingungen; Angemessenheitsentscheide, Standardvertragsklauseln, Data Privacy Framework oder andere anerkannte Garantien, soweit anwendbar.
Odoo S.A. Chaussée de Namur 40 1367 Grand-Rosière, Belgien (nur soweit durch Binadoodoo beauftragt)	Odoo Online / Odoo.sh Plattform, Hosting, Support, Upgrade und Sicherungen im vereinbarten Umfang.	Gewählte Hostingregion sowie weitere Standorte und Unterauftragsbearbeiter gemäss den jeweils geltenden Odoo-Vertragsunterlagen.	Odoo-Datenschutz- und Vertragsbedingungen; Angemessenheitsentscheide, anerkannte Standardvertragsklauseln oder andere zulässige Garantien, soweit erforderlich.
[Name, vollständige Anschrift und UID]	[Weitere Leistung / Rolle]	[Sitz, Hostingort und regelmässige Zugriffsstaaten]	[Vertragliche Grundlage, Angemessenheit, SCC oder andere Garantie]

Direkt durch den Auftraggeber beauftragte Anbieter

Anbieter	Rolle / Leistung	Vertragliche Grundlage beim Auftraggeber
Odoo S.A.	Direkter Plattform- und Hostinganbieter des Auftraggebers	Direktvertrag / DPA / ausgewählte Hostingregion des Auftraggebers
[Weiterer Anbieter]	[Leistung]	[Direktvertrag / DPA / Speicherort]

Änderungsinformation

Binadoodoo kündigt neue oder ersetzte direkte Unterauftragsbearbeiter und zusätzliche regelmässige Zugriffsstaaten gemäss Ziffer 5 mindestens 14 Kalendertage vor dem erstmaligen Einsatz an. Der Auftraggeber hält seine Kontaktangaben aktuell. Frühere Versionen des Online-Verzeichnisses werden archiviert.