Auftragsverarbeitungsvertrag (AVV) für Ordiso Plan

Stand: 24.05.2026
Version: 2026-05-24
Anbieter: Ordiso Plan GbR, Otto-Drescher-Straße 13, 97529 Sulzheim
Vertreten durch: Aurel Plettner und Philipp Schmidt
Kontakt: kontakt@ordiso-plan.de

Diese Seite enthält den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO einschließlich der technischen und organisatorischen Maßnahmen, der Unterauftragsverarbeiterliste sowie der Regelungen zu Datenexport und Löschung.

Der AVV gilt zwischen der **Ordiso Plan GbR** als Auftragnehmer und dem jeweiligen Kunden als Auftraggeber, soweit der AVV im Angebot, Vertrag, in den AGB, in der Auftragsbestätigung oder im Rahmen der Nutzung von Ordiso Plan einbezogen wird.

---

1. Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

1.1 Parteien

Dieser Auftragsverarbeitungsvertrag wird geschlossen zwischen dem jeweiligen Kunden von Ordiso Plan als **Auftraggeber** und

Ordiso Plan GbR
Otto-Drescher-Straße 13
97529 Sulzheim
vertreten durch Aurel Plettner und Philipp Schmidt
E-Mail: kontakt@ordiso-plan.de

als **Auftragnehmer**.

Der Auftraggeber und der Auftragnehmer werden gemeinsam als „Parteien“ bezeichnet.

1.2 Gegenstand und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber die cloudbasierte B2B-Software **Ordiso Plan** zur Verfügung. Ordiso Plan ist eine WebApp/PWA für Handwerks- und Bauunternehmen, insbesondere zur Unterstützung von Projektverwaltung, Einsatzplanung, Zeiterfassung, Baustellen- und Projektdokumentation, Projektkommunikation, Dokumentenerstellung, Angeboten, Rechnungen, Nachkalkulation, Stammdatenverwaltung, Datei-Uploads und mobiler Nutzung.

Je nach gebuchtem Paket, Entwicklungsstand, Konfiguration und aktivierten Funktionen können weitere Funktionen bereitgestellt werden, etwa Eingangsrechnungsverarbeitung, OCR-/KI-gestützte Belegauswertung, DATEV-Export, E-Rechnungsformate, GAEB-/DATANORM-Funktionen, E-Mail-Integrationen, Kalenderfunktionen oder weitere Import-/Exportfunktionen. Diese Funktionen sind nur

Bestandteil der Verarbeitung, soweit sie vom Auftraggeber genutzt, aktiviert oder vertraglich vereinbart werden.

Im Rahmen der Nutzung der Software verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber bleibt Verantwortlicher im Sinne der DSGVO. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach Maßgabe dieses AVV, der Hauptvereinbarung, der Leistungsbeschreibung und dokumentierter Weisungen des Auftraggebers.

Der Auftragnehmer entscheidet nicht eigenständig über Zwecke und Mittel der Verarbeitung der Kundendaten, soweit er als Auftragsverarbeiter tätig wird.

1.3 Art und Zweck der Verarbeitung

Die Verarbeitung kann je nach Nutzung insbesondere folgende Vorgänge umfassen:

- Speicherung, Anzeige, Bearbeitung und Übermittlung von Stammdaten;
- Verwaltung von Nutzern, Rollen, Berechtigungen und Zugängen;
- Projektverwaltung und Projektkommunikation;
- Einsatzplanung, Kalender-, Plantafel- und Ressourcenfunktionen;
- Erfassung, Prüfung und Auswertung von Arbeitszeiten;
- Verwaltung von Abwesenheiten, Urlaubsanträgen und Freigaben, soweit genutzt;
- Dokumentation von Baustellen, Fotos, Checklisten, Berichten und Signaturen;
- Erstellung, Bearbeitung und Speicherung kaufmännischer Dokumente wie Angebote, Rechnungen, Nachträge, Gutschriften und Mahnungen;
- Upload, Speicherung und Verwaltung von Dateien, Anhängen, Fotos, Belegen und Dokumenten;
- Import, Verarbeitung und Archivierung von Eingangsrechnungen, soweit genutzt;
- OCR-/KI-gestützte Auswertung von Eingangsrechnungen, soweit aktiviert oder vereinbart;
- Exportfunktionen, z. B. CSV, XLSX, PDF, DATEV, XRechnung, ZUGFeRD, GAEB oder vergleichbare Formate, soweit verfügbar und genutzt;
- Versand von E-Mails und Benachrichtigungen im Rahmen der Softwarefunktionen, soweit eingerichtet;
- Erstellung von Backups, Systemprotokollen, Fehlerprotokollen und Sicherheitsprotokollen;
- Support, Wartung, Fehleranalyse und technische Betreuung.

1.4 Kategorien betroffener Personen

Je nach Nutzung durch den Auftraggeber können insbesondere folgende Personengruppen betroffen sein:

- Mitarbeiter, Beschäftigte, Subunternehmer und freie Mitarbeiter des Auftraggebers;
- Kunden, Interessenten und Ansprechpartner des Auftraggebers;
- Lieferanten, Dienstleister und Geschäftspartner des Auftraggebers;
- Projektbeteiligte, Bauleiter, Planer, Architekten und Auftraggeber des Auftraggebers;
- Nutzer der WebApp/PWA;
- Empfänger und Absender von E-Mails, Dokumenten, Freigaben und Projektkommunikation.

1.5 Kategorien personenbezogener Daten

Je nach Nutzung verarbeitet Ordiso Plan insbesondere folgende Datenkategorien:

- **Stammdaten:** Name, Firma, Anschrift, E-Mail-Adresse, Telefonnummer, Kundennummer, Lieferantendaten, Ansprechpartnerdaten;
- **Nutzerdaten:** Name, Login-E-Mail, Rolle, Berechtigungen, Status, Einladungsstatus, Login- und Sicherheitsinformationen;
- **Beschäftigtendaten:** interne Personalnummer, Rolle/Tätigkeit, Arbeitszeitmodell, Arbeitszeiten, Urlaubs- und Abwesenheitsdaten, Zeitbuchungen, Freigaben, Korrekturen;
- **Projektdaten:** Projektname, Projektadresse, Projektstatus, Termine, Ressourcen, Notizen, Aufgaben, interne Hinweise;
- **Kommunikationsdaten:** Projektchat, Kommentare, Nachrichteninhalte, Anhänge, Zeitstempel;
- **Dokumentdaten:** Angebote, Rechnungen, Nachträge, Berichte, Checklisten, Signaturen, PDF-Dateien, E-Rechnungsdaten, GAEB-/DATEV-Daten, soweit genutzt;
- **Datei- und Mediendaten:** Fotos, Uploads, Anhänge, Belege, Signaturen;
- **Rechnungs- und Zahlungsdaten:** Rechnungsnummern, Beträge, Zahlungsstatus, Zahlungsziele, Bankdaten des Auftraggebers oder seiner Kunden, soweit vom Auftraggeber eingegeben;
- **Technische Daten:** IP-Adressen, Logdaten, Geräte- und Browserinformationen, Fehlermeldungen, Session- und Sicherheitsereignisse.

Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO sind nicht Gegenstand der vereinbarten Standardnutzung. Der Auftraggeber ist angewiesen, solche Daten nicht in Freitextfelder, Chats, Notizen oder Uploads einzugeben, soweit dies nicht für die Nutzung ausdrücklich erforderlich und rechtlich zulässig ist.

Soweit der Auftraggeber in der Software Abwesenheiten wie Krankheit, Krankmeldung oder vergleichbare gesundheitsnahe Angaben erfasst, entscheidet der Auftraggeber über Rechtsgrundlage, Umfang, Information der Betroffenen und Berechtigungskonzept. Ordiso Plan verarbeitet solche Daten ausschließlich technisch im Rahmen der bereitgestellten Funktionen und nach Weisung des Auftraggebers.

1.6 Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer der Hauptvereinbarung über die Nutzung von Ordiso Plan.

Nach Vertragsende werden personenbezogene Daten nach Maßgabe der Hauptvereinbarung, dieses AVV und des Datenexport-, Anbieterwechsel- und Löschkonzepts gelöscht, anonymisiert oder zurückgegeben, soweit keine gesetzlichen Pflichten, berechtigten Nachweisinteressen oder vereinbarten Übergangsfristen entgegenstehen.

Daten in Backups und technischen Sicherungen werden nicht zwingend sofort einzeln gelöscht, sondern nach den vorgesehenen Backup- und Löschzyklen gelöscht oder überschrieben. Der Zugriff auf Backups ist beschränkt und erfolgt grundsätzlich nur zu Wiederherstellungszwecken.

1.7 Weisungen des Auftraggebers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers.

Weisungen ergeben sich insbesondere aus:

- der Hauptvereinbarung;
- diesem AVV;
- der Nutzung der Softwarefunktionen durch berechtigte Nutzer;
- den vom Auftraggeber vorgenommenen Einstellungen, Uploads, Exporten und Freigaben;
- schriftlichen oder textförmlichen Einzelweisungen des Auftraggebers.

Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Der Auftragnehmer ist berechtigt, die Durchführung einer offensichtlich rechtswidrigen Weisung bis zur Klärung auszusetzen.

1.8 Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich insbesondere:

- personenbezogene Daten nur im Rahmen dieses AVV und dokumentierter Weisungen zu verarbeiten;
- geeignete technische und organisatorische Maßnahmen gemäß Anlage TOMs umzusetzen und aufrechtzuerhalten;
- Personen, die Zugriff auf personenbezogene Daten haben, zur Vertraulichkeit zu verpflichten;
- den Auftraggeber bei der Erfüllung von Betroffenenrechten angemessen zu unterstützen;
- den Auftraggeber bei Datenschutz-Folgenabschätzungen und Konsultationen mit Aufsichtsbehörden angemessen zu unterstützen, soweit dies die Auftragsverarbeitung betrifft;
- Datenschutzverletzungen dem Auftraggeber unverzüglich nach Bekanntwerden zu melden, soweit Kundendaten betroffen sind;
- Unterauftragsverarbeiter nur nach Maßgabe dieses AVV einzusetzen;
- nach Vertragsende Daten nach Maßgabe dieses AVV und der vereinbarten Export- und Löschregelungen zurückzugeben oder zu löschen, soweit keine gesetzlichen Pflichten oder berechtigten Nachweisinteressen entgegenstehen;
- erforderliche Nachweise über die Einhaltung der Pflichten bereitzustellen.

1.9 Pflichten des Auftraggebers

Der Auftraggeber ist insbesondere verantwortlich für:

- die Rechtmäßigkeit der Verarbeitung der von ihm eingegebenen personenbezogenen Daten;
- die Information betroffener Personen;
- die Einholung erforderlicher Einwilligungen, soweit erforderlich;
- die Einrichtung, Prüfung und Pflege von Rollen, Berechtigungen und Nutzerkonten;
- die Prüfung, welche personenbezogenen Daten in Ordiso Plan eingegeben werden dürfen;
- die Beachtung arbeitsrechtlicher, steuerlicher, handelsrechtlicher und branchenspezifischer Aufbewahrungs- und Dokumentationspflichten;
- die sachliche Richtigkeit der Kundendaten, Mitarbeiterdaten, Projektinformationen und Dokumentinhalte;
- die Prüfung, ob besondere Kategorien personenbezogener Daten verarbeitet werden dürfen und welche zusätzlichen Schutzmaßnahmen hierfür erforderlich sind.

1.10 Technische und organisatorische Maßnahmen

Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage „Technische und organisatorische Maßnahmen“.

Der Auftragnehmer darf die TOMs weiterentwickeln und ändern, sofern das Schutzniveau nicht wesentlich unterschritten wird. Wesentliche Änderungen, die das Schutzniveau relevant beeinflussen, werden dokumentiert.

1.11 Unterauftragsverarbeiter

Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz der in der Anlage „Unterauftragsverarbeiterliste“ genannten Unterauftragsverarbeiter.

Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen hinsichtlich Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern in angemessener Weise, z. B. per E-Mail, In-App-Hinweis oder über eine aktualisierte Unterauftragsverarbeiterliste.

Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen. Erfolgt kein Widerspruch innerhalb von 14 Tagen nach Mitteilung, gilt die Änderung als genehmigt.

Der Auftragnehmer schließt mit Unterauftragsverarbeitern Vereinbarungen, die ein angemessenes Datenschutzniveau sicherstellen und die gesetzlichen Anforderungen an Auftragsverarbeitung erfüllen, soweit der jeweilige Dienstleister als Auftragsverarbeiter eingesetzt wird.

1.12 Drittlandübermittlungen

Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, soweit die Voraussetzungen der DSGVO erfüllt sind.

Soweit Unterauftragsverarbeiter oder deren verbundene Unternehmen Daten in Drittländern verarbeiten, werden geeignete Garantien eingesetzt, insbesondere Angemessenheitsbeschlüsse, EU-Standardvertragsklauseln oder andere zulässige Mechanismen.

Die konkrete Einordnung ergibt sich aus der Unterauftragsverarbeiterliste und den Informationen der jeweiligen Dienstleister.

1.13 Unterstützung bei Betroffenenrechten

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren und technisch Möglichen bei der Erfüllung von Rechten betroffener Personen, insbesondere Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.

Geht eine Anfrage einer betroffenen Person unmittelbar beim Auftragnehmer ein und betrifft sie Kundendaten des Auftraggebers, leitet der Auftragnehmer die Anfrage an den Auftraggeber weiter, soweit eine Zuordnung möglich ist.

Der Auftragnehmer beantwortet solche Anfragen nicht eigenständig inhaltlich, soweit er als Auftragsverarbeiter tätig ist, es sei denn, er ist hierzu gesetzlich verpflichtet.

1.14 Datenschutzverletzungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, soweit diese Kundendaten betrifft.

Die Mitteilung erfolgt an die vom Auftraggeber hinterlegte oder benannte Kontaktadresse. Der Auftraggeber ist dafür verantwortlich, eine aktuelle Kontaktadresse zu hinterlegen.

Die Mitteilung enthält, soweit verfügbar:

- Art der Datenschutzverletzung;
- betroffene Datenarten und Systeme;
- betroffene oder voraussichtlich betroffene Personengruppen;
- wahrscheinliche Folgen;
- bereits ergriffene oder vorgeschlagene Maßnahmen;
- Ansprechpartner für Rückfragen.

Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung gesetzlicher Melde- und Benachrichtigungspflichten.

1.15 Kontrollrechte und Nachweise

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage geeignete Informationen zum Nachweis der Einhaltung dieses AVV zur Verfügung.

Kontrollen erfolgen vorrangig durch Dokumentation, Selbstauskünfte, Sicherheitskonzepte, Zertifikate oder sonstige geeignete Nachweise.

Vor-Ort-Prüfungen sind nur nach vorheriger Abstimmung, während üblicher Geschäftszeiten, ohne Störung des Betriebs und unter Wahrung von Sicherheits- und Vertraulichkeitsinteressen zulässig.

Der Auftraggeber trägt eigene Kosten der Prüfung. Zusätzlicher Aufwand des Auftragnehmers kann nach vorheriger Abstimmung angemessen berechnet werden.

1.16 Löschung und Rückgabe nach Vertragsende

Nach Vertragsende stellt der Auftragnehmer dem Auftraggeber nach Maßgabe des Datenexport-, Anbieterwechsel- und Löschkonzepts Exportmöglichkeiten bereit.

Nach Ablauf der vereinbarten Export- und Übergangsfristen werden Kundendaten gelöscht oder anonymisiert, soweit keine gesetzlichen Pflichten, berechtigten Nachweisinteressen oder technische Backup-Zyklen entgegenstehen.

Daten in Backups werden nach den vorgesehenen Backup-Zyklen gelöscht oder überschrieben.

Der Auftraggeber bleibt für die Erfüllung eigener handels-, steuer-, arbeits- und branchenspezifischer Aufbewahrungspflichten verantwortlich. Ordiso Plan ersetzt kein revisionssicheres Archivsystem, soweit dies nicht ausdrücklich vereinbart wurde.

1.17 Haftung

Die Haftung richtet sich nach den Regelungen der Hauptvereinbarung, soweit gesetzlich zulässig. Gesetzliche Ansprüche nach der DSGVO bleiben unberührt.

1.18 Rangfolge

Bei Widersprüchen gilt folgende Rangfolge:

1. individuelle Vereinbarungen der Parteien;
2. dieser AVV einschließlich Anlagen;
3. Hauptvertrag / AGB;
4. Leistungsbeschreibung.

1.19 Schlussbestimmungen

Änderungen und Ergänzungen dieses AVV bedürfen der Textform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist.

Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Es gilt deutsches Recht.

---

2. Anlage: Technische und organisatorische Maßnahmen (TOMs)

Anbieter: Ordiso Plan GbR
Produkt: Ordiso Plan WebApp/PWA
Stand: 24.05.2026

Die nachfolgenden technischen und organisatorischen Maßnahmen beschreiben den aktuellen organisatorischen und technischen Schutzstandard für Ordiso Plan. Die Maßnahmen werden risikoorientiert weiterentwickelt.

2.1 Vertraulichkeit

Zutrittskontrolle

Ordiso Plan betreibt keine eigenen Rechenzentren. Hosting und Infrastruktur erfolgen über professionelle Cloud-Dienstleister. Physische Zutrittskontrollen zu Rechenzentren werden durch die jeweiligen Infrastruktur-Dienstleister umgesetzt.

Interne Arbeitsplätze und Geräte werden durch angemessene organisatorische Maßnahmen geschützt, insbesondere:

- Zugriff auf Arbeitsgeräte nur durch berechtigte Personen;
- Bildschirmsperre bei Abwesenheit;
- Schutz vor unbefugter Einsichtnahme;
- Nutzung individueller Benutzerkonten.

Zugangskontrolle

- Zugriff auf die WebApp erfolgt über individuelle Benutzerkonten.
- Nutzer erhalten rollenbasierte Berechtigungen, z. B. Chef, Büro, Worker/Mobil.
- Passwörter werden nicht im Klartext gespeichert.
- Sitzungen werden serverseitig verwaltet und können beendet werden.
- Kritische Bereiche sind nur für berechtigte Rollen zugänglich.
- Administrative Zugänge zu Infrastruktur- und Dienstleisterkonten werden auf notwendige Personen beschränkt.
- Der Zugriff auf zentrale Infrastruktur- und Administrationskonten wird auf notwendige Personen beschränkt und durch individuelle Konten, starke Passwörter, rollenbasierte Zugriffsbeschränkungen und die Sicherheitsmechanismen der jeweiligen Anbieter geschützt.
- Eine verpflichtende Zwei-Faktor-Authentisierung für App-Nutzer ist derzeit nicht Bestandteil der Standardfunktionen.
- Zwei-Faktor-Authentisierung für interne Administratoren und privilegierte Kundenrollen ist als Weiterentwicklung vorgesehen, soweit dies technisch und organisatorisch umgesetzt wird.

Zugriffskontrolle

- Mandantentrennung auf Anwendungsebene: Nutzer dürfen nur Daten ihrer Organisation einsehen, soweit keine besondere interne Berechtigung besteht.
- Serverseitige Zugriffskontrollen für API-Routen.
- Rollen- und Rechtekonzept für Projekt-, Dokument-, Zeit-, Personal- und Adminfunktionen.
- Zugriff auf Rechnungen, DATEV-Exporte, Mitarbeiterdaten, Kostenwerte und Einstellungen nur für berechtigte Rollen.
- Berechtigungen werden bei relevanten Aktionen serverseitig geprüft.
- Direkte Dateiabrufe erfolgen nur nach Authentifizierungs- und Berechtigungsprüfung oder über zeitlich beschränkte Zugriffsmöglichkeiten.

Trennungskontrolle

- Daten verschiedener Kundenorganisationen werden logisch getrennt.
- Mandantenbezug wird bei Datenbankabfragen und API-Operationen berücksichtigt.
- Produktiv-, Entwicklungs- und Testumgebungen werden getrennt gehalten, soweit praktisch umsetzbar.
- Testdaten sollen keine produktiven personenbezogenen Daten enthalten, sofern dies nicht notwendig und abgesichert ist.

Verschlüsselung und Secret-Management

- Datenübertragung erfolgt grundsätzlich verschlüsselt über HTTPS/TLS.
- Datenbank- und Speicheranbieter setzen serverseitige Sicherheitsmaßnahmen ein.
- Secrets, API-Keys und Zugangsdaten werden nicht im Quellcode gespeichert, sondern über Umgebungsvariablen bzw. Secret-Verwaltung bereitgestellt.
- Sensible Umgebungsvariablen werden in Deployment-Systemen als geschützte Variablen geführt.

2.2 Integrität

Eingabekontrolle und Protokollierung

- Relevante Systemereignisse werden protokolliert, z. B. Logins, Fehler, API-Zugriffe, sicherheitsrelevante Aktionen und administrative Änderungen, soweit technisch implementiert.
- Kritische Geschäftsobjekte wie finalisierte Rechnungen sollen nicht still überschrieben werden.
- Dokumente und Rechnungen werden mit Versions- und Statuskonzepten verarbeitet.
- Für finalisierte Dokumente werden Snapshots bzw. exportierte Dateien gespeichert, soweit die Funktion aktiviert ist.

Fehler- und Manipulationsschutz

- Servervalidierungen für kritische Aktionen.
- Validierung von Datei-Uploads nach Dateityp und Größe.
- Berechtigungsprüfung vor Exporten, Downloads und Dokumentfreigaben.
- Schutz vor unbefugtem Zugriff auf API-Routen.
- Einsatz von CSRF-Schutz, soweit für mutierende Webaktionen erforderlich.
- Protokollierung von Fehlern zur Analyse und Verbesserung.

Änderungskontrolle

- Änderungen am Quellcode erfolgen versioniert.
- Deployments erfolgen über definierte Deployment-Prozesse.
- Änderungen an Produktionsumgebungen werden nachvollziehbar verwaltet.
- Datenbankmigrationen werden versioniert und vor produktiver Nutzung getestet, soweit praktisch möglich.

2.3 Verfügbarkeit und Belastbarkeit

Hosting und Betrieb

- Die Anwendung wird über Vercel betrieben.
- Die Datenbank wird über Neon Postgres betrieben, nach Möglichkeit mit Region Frankfurt bzw. EU-naher Region.
- Dateiablage erfolgt für produktive Uploads über privaten Object Storage, insbesondere Cloudflare R2, soweit aktiviert.
- Systemmails können über Resend, Google Workspace/Gmail API oder kundenseitige Mailanbindungen versendet werden, soweit eingerichtet.

Backups und Wiederherstellung

- Datenbank-Backups bzw. Point-in-Time-Restore-Funktionen werden über den Datenbankanbieter bereitgestellt.
- Die konkreten Backup- und Restore-Zeiträume richten sich nach dem jeweils eingesetzten Infrastruktur- und Datenbanktarif.
- Restore-Prozesse sollen regelmäßig getestet werden, insbesondere vor oder nach größeren Datenbankänderungen.
- Dateien im Object Storage sind gesondert von der Datenbank zu betrachten. Ein Datenbank-Restore stellt nicht automatisch gelöschte Dateien wieder her, soweit diese extern gespeichert sind.

Verfügbarkeit

- Ordiso Plan wird mit angemessener Sorgfalt betrieben.
- Eine feste Verfügbarkeitsgarantie wird nicht vereinbart, sofern sie nicht ausdrücklich in einer gesonderten Vereinbarung zugesagt wird.
- Wartungen, Updates und Sicherheitsmaßnahmen dürfen durchgeführt werden, soweit zumutbar und erforderlich.
- Störungen werden nach Priorität bearbeitet.

2.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Regelmäßige Prüfung von Rollen- und Berechtigungskonzepten.
- Regelmäßige Aktualisierung von Abhängigkeiten und Sicherheitsupdates, soweit praktikabel.
- Überwachung von Fehlern und Systemverhalten.
- Prüfung von Backup- und Restore-Fähigkeit.
- Prüfung von Dateiablage, Zugriffsrechten und Exportfunktionen.
- Dokumentation relevanter Änderungen an Sicherheits- und Datenschutzmaßnahmen.

2.5 Datenschutzfreundliche Voreinstellungen

- Rollenbasierte Rechtevergabe.
- Grundsatz der Datenminimierung bei Formularen und Anzeigen.
- Sensible Bereiche, z. B. Mitarbeiterkosten, Exportfunktionen, Bankdaten und DATEV-Exporte, werden nur für berechtigte Rollen angezeigt.
- Uploads werden privat gespeichert, sofern nicht ausdrücklich anders konfiguriert.
- Keine öffentliche Freigabe von Projektdateien ohne entsprechende Funktion und Berechtigungsprüfung.
- PWA- und Offline-Daten werden nur soweit gespeichert, wie dies für Offline-Funktionen erforderlich ist.

2.6 Aufbewahrung und Löschung

Regellöschfristen gelten, soweit technisch umgesetzt, vertraglich vereinbart und keine gesetzlichen Pflichten oder berechtigten Nachweisinteressen entgegenstehen.

- Nutzerkonten: Deaktivierung nach Vertragsende oder Offboarding; Löschung oder Anonymisierung personenbezogener Kontodaten nach angemessener Frist, soweit keine Pflichten entgegenstehen.
- Projekt-, Chat-, Zeit- und Dokumentationsdaten: Löschung oder Anonymisierung nach Vertragsende und Ablauf vereinbarter Export- und Übergangsfristen, soweit keine Nachweis-, Gewährleistungs-, Verjährungs- oder Aufbewahrungsgründe entgegenstehen.
- Uploads, Fotos, Signaturen, Anhänge: Löschung nach Projekt- oder Vertragsende, soweit keine gesetzlichen oder berechtigten Aufbewahrungsinteressen bestehen.
- Error-Logs: grundsätzlich zeitlich begrenzt, soweit technisch steuerbar.
- Rate-Limit- und Sicherheitsdaten: grundsätzlich zeitlich begrenzt, soweit technisch steuerbar.
- Audit-Logs: Aufbewahrung entsprechend dem jeweiligen Sicherheits- und Nachweiszweck.
- Backups: Löschung oder Überschreibung nach den technischen Backup-Zyklen der eingesetzten Infrastruktur.
- Steuerlich oder handelsrechtlich relevante Unterlagen: nach den jeweils anwendbaren gesetzlichen Vorgaben durch den hierfür verantwortlichen Vertragspartner.

2.7 Mitarbeiter und Vertraulichkeit

- Personen mit Zugriff auf personenbezogene Daten werden zur Vertraulichkeit verpflichtet.
- Zugriffe werden nach dem Need-to-know-Prinzip vergeben.
- Externe Dienstleister und Freelancer erhalten Zugriff nur, soweit erforderlich und vertraglich abgesichert.
- Zugänge werden bei Ausscheiden oder Wegfall der Erforderlichkeit entzogen.

---

3. Anlage: Unterauftragsverarbeiterliste

Anbieter: Ordiso Plan GbR
Produkt: Ordiso Plan WebApp/PWA
Stand: 24.05.2026

Der Auftragnehmer setzt die nachfolgenden Unterauftragsverarbeiter ein. Die konkrete Verarbeitung über einzelne Dienste kann je nach Tarif, Konfiguration und aktivierten Funktionen variieren. Dienste, die nur für bestimmte Funktionen erforderlich sind, verarbeiten Daten nur, soweit die jeweilige Funktion genutzt, aktiviert oder angebunden wird.

3.1 Regelmäßig eingesetzte Unterauftragsverarbeiter

Dienstleister	Zweck	Mögliche Datenarten	Sitz / Verarbeitung	Bemerkung
Vercel Inc.	Hosting, Deployment, Auslieferung der WebApp, Serverless Functions, Analytics/Speed Insights	IP-Adressen, technische Logdaten, Nutzungs- und Performance-Daten, Anwendungsdaten bei API-Verarbeitung	USA / weltweit, EU-nahe Konfiguration soweit möglich	Hosting der Anwendung und technischer Betrieb
Neon, Inc. / Neon-Dienst	PostgreSQL-Datenbank	Stammdaten, Projekt-, Nutzer-, Zeit-, Dokument- und Rechnungsdaten	Region nach Projektkonfiguration, vorgesehen Frankfurt/EU	Datenbankbetrieb
Cloudflare, Inc.	Cloudflare R2 Object Storage, DNS-, Sicherheits- und Netzwerkdienste, soweit genutzt	Uploads, Dateien, PDFs, Fotos, Anhänge, technische Zugriffsdaten	EU-Jurisdiction für R2, soweit konfiguriert; sonst gemäß Dienstleisterangaben	Private Dateiablage / Object Storage und technische Infrastruktur

Dienstleister	Zweck	Mögliche Datenarten	Sitz / Verarbeitung	Bemerkung
Resend, Inc.	Versand von System- und Plattform-E-Mails	Empfänger- und Absenderadressen, Betreff, E-Mail-Inhalte, Zustell- und Fehlerdaten	USA / gemäß Anbieterangaben	Transaktionale E-Mails, soweit genutzt

3.2 Weitere Unterauftragsverarbeiter und Integrationen je nach aktivierter Funktion

Dienstleister	Zweck	Mögliche Datenarten	Sitz / Verarbeitung	Bemerkung
Google Ireland Ltd. / Google LLC	Google Workspace, Gmail API, Google Calendar/Meet, Google Document AI	E-Mail-Adressen, E-Mail-Inhalte, Kalenderdaten, Rechnungs- und Beleginhalte bei OCR-/KI-Verarbeitung, technische Daten	EU/USA/weltweit gemäß Google-Vertragsbedingungen	E-Mail, Kalender und KI-/OCR-gestützte Eingangsrechnungsverarbeitung, soweit die jeweilige Funktion genutzt oder angebunden wird
Microsoft Ireland Operations Limited / Microsoft Corporation	Microsoft-365-/ Outlook-E-Mail-Versand, Microsoft Graph, OAuth-Anbindung, Kalenderfunktionen	E-Mail-Adressen, E-Mail-Inhalte, Kalenderdaten, technische OAuth-/Token-Daten	EU/USA/weltweit gemäß Microsoft-Vertragsbedingungen	Microsoft-365-Integration, soweit vom Auftraggeber aktiviert oder angebunden
Weitere im Angebot oder in der App benannte Dienstleister	Zusatzfunktionen, Integrationen oder kundenseitige Anbindungen	Je nach Funktion	Je nach Anbieter	Nur soweit vertraglich vereinbart, aktiviert oder technisch erforderlich

3.3 Hinweise

- Der Auftragnehmer informiert über wesentliche Änderungen der Unterauftragsverarbeiterliste in angemessener Weise.
- Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Tagen nach Mitteilung widersprechen.
- Soweit Daten außerhalb der EU/des EWR verarbeitet werden, werden geeignete Garantien eingesetzt, insbesondere Angemessenheitsbeschlüsse, Standardvertragsklauseln oder andere zulässige Mechanismen.

- Dienste, die nur optional genutzt werden, verarbeiten Daten nur, wenn die entsprechende Funktion aktiviert, angebunden oder technisch erforderlich ist.
- Zahlungsdienstleister, Bankdienstleister oder Anbieter für die Abwicklung der Vertragsbeziehung zwischen Ordiso Plan und dem Kunden sind nicht automatisch Unterauftragsverarbeiter für die Verarbeitung der vom Kunden in Ordiso Plan eingegebenen Projektdaten. Sie können jedoch in Datenschutzhinweisen für die eigene Vertrags- und Zahlungsabwicklung von Ordiso Plan gesondert genannt werden.

---

4. Anlage: Datenexport-, Anbieterwechsel- und Löschkonzept

Anbieter: Ordiso Plan GbR
Produkt: Ordiso Plan WebApp/PWA
Stand: 24.05.2026

4.1 Ziel

Dieses Konzept beschreibt, wie Kunden ihre Daten aus Ordiso Plan exportieren, einen Anbieterwechsel vorbereiten und Daten nach Vertragsende löschen oder anonymisieren lassen können.

4.2 Datenexport während der Vertragslaufzeit

Der Kunde kann während der Vertragslaufzeit je nach Funktionsumfang Daten exportieren, insbesondere:

- Kunden-, Lieferanten- und Kontaktstammdaten als CSV/XLSX;
- Projektlisten und Projektdaten als CSV/XLSX oder PDF;
- Zeitdaten als CSV/XLSX oder PDF-Bericht;
- Angebote, Rechnungen, Nachträge, Mahnungen und andere Dokumente als PDF;
- E-Rechnungen als XRechnung/ZUGFeRD, soweit unterstützt;
- DATEV-Exportpakete, soweit unterstützt;
- GAEB-Dateien, soweit unterstützt;
- Eingangsrechnungsarchiv als ZIP/CSV, soweit unterstützt;
- Dokumentationsberichte, Fotos, Checklisten und Projektanhänge, soweit unterstützt.

Der genaue Exportumfang hängt vom gebuchten Paket, den aktivierten Funktionen und der technischen Verfügbarkeit ab.

4.3 Datenexport nach Vertragsende

Nach Vertragsende stellt Ordiso Plan dem Kunden auf Anfrage für einen angemessenen Zeitraum Exportmöglichkeiten bereit.

Sofern nicht abweichend vereinbart, stehen Exportmöglichkeiten bis 30 Tage nach Vertragsende zur Verfügung. Danach kann der Zugang deaktiviert und die Löschung oder Anonymisierung eingeleitet werden, soweit keine gesetzlichen Pflichten, berechtigten Nachweisinteressen oder technische Backup-Zyklen entgegenstehen.

4.4 Anbieterwechsel

Zur Unterstützung eines Anbieterwechsels kann Ordiso Plan insbesondere bereitstellen:

- strukturierte Exporte gängiger Datenkategorien;
- PDF-/ZIP-Archive relevanter Dokumente;
- Hinweise zu Datenformaten;
- technische Unterstützung nach Aufwand, soweit vereinbart.

Eine vollständige Kompatibilität mit Systemen anderer Anbieter wird nicht garantiert. Individuelle Migrationen, Sonderformate oder Datenbereinigungen sind gesondert zu vereinbaren.

4.5 Löschung nach Vertragsende

Nach Ablauf der Exportfrist werden Kundendaten gelöscht oder anonymisiert, soweit keine gesetzlichen Pflichten, berechtigten Nachweisinteressen oder technische Backup-Zyklen entgegenstehen.

Empfohlene Logik:

- Nutzerzugänge: Deaktivierung zum Vertragsende; Löschung oder Anonymisierung personenbezogener Nutzerkontodaten nach angemessener Frist, soweit nicht erforderlich.
- Projekt- und Dokumentdaten: Löschung oder Anonymisierung nach Ablauf der Exportfrist, soweit keine Nachweis- oder Aufbewahrungsgründe bestehen.
- Uploads, Fotos, Anhänge, Signaturen: Löschung nach Ablauf der Exportfrist, soweit keine Aufbewahrungspflichten bestehen.
- Chat- und Kommunikationsdaten: Löschung oder Anonymisierung nach Ablauf relevanter Nachweisfristen.
- Logs: Löschung nach definierten Logfristen, soweit technisch steuerbar.
- Backups: Löschung oder Überschreibung nach technischen Backup-Zyklen.

Der Auftraggeber bleibt für die Erfüllung eigener handels-, steuer-, arbeits- und branchenspezifischer Aufbewahrungspflichten verantwortlich. Ordiso Plan stellt hierfür während der Vertragslaufzeit und für die vereinbarte Exportfrist Exportmöglichkeiten bereit. Eine dauerhafte Archivierung nach Vertragsende wird nur geschuldet, wenn dies ausdrücklich vereinbart wurde.

Ordiso Plan ersetzt kein revisionssicheres Archivsystem, soweit dies nicht ausdrücklich vereinbart wurde.

4.6 Löschung einzelner Daten während der Vertragslaufzeit

Der Kunde kann im Rahmen der Softwarefunktionen einzelne Daten löschen oder archivieren. Bei bestimmten Daten, insbesondere finalisierten Rechnungen, Audit-Logs, Exportnachweisen oder steuerlich relevanten Unterlagen, kann eine Löschung eingeschränkt sein.

4.7 Backups

Daten in Backups werden nicht unmittelbar einzeln gelöscht, sondern im Rahmen der festgelegten Backup-Zyklen überschrieben oder gelöscht. Bis dahin ist der Zugriff auf Backups beschränkt und erfolgt nur zu Wiederherstellungszwecken.

4.8 Löschbestätigung

Auf Anfrage kann Ordiso Plan dem Kunden nach Abschluss der Löschung eine Bestätigung in Textform bereitstellen. Diese Bestätigung bezieht sich nicht auf Daten, die aufgrund gesetzlicher Pflichten, berechtigter Nachweisinteressen oder laufender Backup-Zyklen noch vorübergehend gespeichert bleiben.

4.9 Verantwortung des Kunden

Der Kunde ist verantwortlich dafür, vor Vertragsende erforderliche Exporte durchzuführen und gesetzliche Aufbewahrungspflichten für eigene Geschäftsunterlagen zu erfüllen.

---

5. Anlage: Support-, Wartungs- und Verfügbarkeitsbeschreibung

Anbieter: Ordiso Plan GbR
Produkt: Ordiso Plan WebApp/PWA
Stand: 24.05.2026

5.1 Supportkanäle

Support wird grundsätzlich über folgende Kanäle erbracht:

- E-Mail: kontakt@ordiso-plan.de;
- In-App-Support oder Feedback-Funktion, soweit verfügbar;
- nach individueller Vereinbarung telefonisch oder per Videotermin.

Ein Anspruch auf telefonischen Support oder bestimmte Reaktionszeiten besteht nur, wenn dies ausdrücklich vereinbart wurde.

5.2 Supportzeiten

Reguläre Supportbearbeitung erfolgt in der Regel Montag bis Freitag zwischen 09:00 und 17:00 Uhr, ausgenommen gesetzliche Feiertage in Bayern. Verbindliche Reaktions- oder Lösungszeiten bestehen nur, wenn sie individuell vereinbart wurden.

5.3 Priorisierung von Anfragen

Supportanfragen werden nach Schwere und Dringlichkeit priorisiert.

Priorität 1 – Kritische Störung
Die Nutzung der Kernfunktionen ist für mehrere Nutzer oder den Kunden insgesamt nicht möglich, z. B. Login-Ausfall, vollständiger Systemausfall oder schwerwiegender Datenzugriffsfehler. Ziel ist eine schnellstmögliche Prüfung und Bearbeitung.

Priorität 2 – Erhebliche Störung
Wichtige Funktionen sind eingeschränkt, es besteht aber ein Workaround, z. B. PDF-Export, E-Mail-Versand, Rechnungsfunktion, Zeiterfassung oder Projektzugriff teilweise gestört. Ziel ist eine zeitnahe Bearbeitung nach Priorität und Kapazität.

Priorität 3 – Normale Anfrage
Fragen zur Bedienung, kleinere Fehler, Verbesserungsvorschläge, Darstellungsprobleme oder nicht kritische Funktionswünsche. Ziel ist eine Bearbeitung nach Eingang, Aufwand und Priorität.

5.4 Wartung und Updates

Ordiso Plan darf Wartungen, Updates, Sicherheitsverbesserungen und Funktionsanpassungen durchführen.

Updates können ohne vorherige Zustimmung des Kunden eingespielt werden, soweit sie den Vertragszweck nicht wesentlich beeinträchtigen.

Geplante Wartungen mit voraussichtlich erheblicher Auswirkung sollen nach Möglichkeit vorab angekündigt werden.

Sicherheitsrelevante Updates können kurzfristig und ohne Vorankündigung durchgeführt werden.

5.5 Verfügbarkeit

Ordiso Plan strebt eine angemessene Verfügbarkeit der WebApp an. Eine bestimmte Mindestverfügbarkeit oder ein verbindliches Service Level Agreement wird nur geschuldet, wenn dies ausdrücklich individuell vereinbart wurde.

Die Verfügbarkeit kann insbesondere beeinträchtigt sein durch:

- Wartungen und Updates;
- Störungen bei Hosting-, Datenbank-, Speicher-, E-Mail-, Netzwerk- oder Drittanbietern;
- höhere Gewalt;
- Angriffe, Missbrauch oder Sicherheitsvorfälle;
- fehlerhafte Konfiguration durch Kunden;
- Ausfälle von Endgeräten, Browsern, Internetverbindungen oder Drittsoftware des Kunden.

5.6 Datensicherungen und Wiederherstellung

Ordiso Plan nutzt Sicherungs- und Wiederherstellungsfunktionen der eingesetzten Infrastruktur- und Datenbankanbieter.

Backups dienen der Wiederherstellung des Betriebs bei technischen Störungen und sind kein Ersatz für kundenseitige Export- oder Archivierungspflichten.

Eine Wiederherstellung einzelner versehentlich gelöschter Datensätze kann nicht in jedem Fall zugesichert werden.

R2-/Object-Storage-Dateien und Datenbankdaten sind technisch getrennt zu betrachten.

5.7 Kundenpflichten bei Support

Der Kunde stellt bei Supportanfragen angemessene Informationen bereit, insbesondere:

- betroffene Organisation / Nutzer;

- Beschreibung des Problems;
- Zeitpunkt und betroffene Funktion;
- Fehlermeldungen oder Screenshots;
- relevante Dokumentnummern oder Projektbezüge;
- bereits getestete Schritte.

5.8 Beta-, Pilot- und Testfunktionen

Neue Funktionen können als Beta-, Pilot- oder Testfunktionen bereitgestellt werden. Solche Funktionen können fehleranfälliger sein, sich ändern oder wieder entfernt werden. Ein Anspruch auf dauerhafte Bereitstellung besteht nur, wenn dies ausdrücklich vereinbart wurde.

---

6. Hinweise zur Einbeziehung und Versionierung

Dieser AVV einschließlich Anlagen kann dem Kunden vor oder bei Vertragsschluss bereitgestellt und über Angebot, Auftragsbestätigung, AGB, Vertragslink oder In-App-Bestätigung einbezogen werden.

Ordiso Plan sollte intern dokumentieren, welche Version des AVV für welchen Kunden galt, insbesondere:

- AVV-Version;
- Datum der Bereitstellung oder Annahme;
- Kunde / Organisation;
- akzeptierende Person, soweit bekannt;
- Einbeziehungsweg, z. B. Angebot, E-Mail, AGB-Link oder In-App-Bestätigung.

Änderungen dieser Seite gelten nicht automatisch rückwirkend, soweit nicht ausdrücklich vereinbart oder gesetzlich zulässig.