orth & kellenberger GROUP

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 DSGVO · Muster der Orth-Kellenberger Group KG für alle Marken · Fassung 1.1 · Stand 2. November 2026 · Veröffentlichungsfassung

> Muster (Veröffentlichungsfassung ohne Namen und Anschriften der Unterauftragsverarbeiter; die vollständige Anlage 3 erhält der Auftraggeber mit dem Vertrag). Platzhalter in eckigen Klammern werden je Vertrag ausgefüllt. Diese Vereinbarung ergänzt den Hauptvertrag (Dienstvertrag, Managed-Services-Vertrag, Hostingvertrag, Partnervertrag, Nutzungsvertrag orandke ONE) und gilt für alle Marken der Orth-Kellenberger Group KG: orandke IT, orandke IT Trainings, orandke ONE, OR-KE, orkenet. Anlagen: 1 Gegenstand der Verarbeitung, 2 Technische und organisatorische Maßnahmen, 3 Unterauftragsverarbeiter, 4 Weisungsberechtigte und Ansprechstellen.

zwischen

[Firma des Auftraggebers], [Straße Hausnummer], [PLZ Ort], vertreten durch [Vorname Nachname, Funktion]

– nachfolgend „Auftraggeber“ –

und der

Orth-Kellenberger Group KG, Pfarrackerstraße 9, 84326 Falkenberg, vertreten durch die persönlich haftende Gesellschafterin Orth-Kellenberger Group Management GmbH, diese vertreten durch die Geschäftsführer Mariam Orth, Tobias Hitzenauer, Jedidjah Orth

– nachfolgend „Auftragnehmer“ –

1 Gegenstand und Dauer

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO. Gegenstand, Art, Zweck und Umfang der Verarbeitung, die Art der Daten und der Kreis der betroffenen Personen ergeben sich aus dem Hauptvertrag [Vertragsnummer/Bezeichnung] vom [Datum] und aus Anlage 1.

1.2 Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags. Sie endet, wenn der Auftragnehmer keine personenbezogenen Daten des Auftraggebers mehr verarbeitet; die Pflichten nach Ziffer 11 (Rückgabe und Löschung) bleiben bis zu ihrer Erfüllung bestehen.

1.3 Die Verarbeitung findet in Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums statt. Eine Verarbeitung in einem Drittland ist nur mit den in Anlage 3 genannten Unterauftragsverarbeitern und unter den Voraussetzungen der Art. 44 ff. DSGVO (Angemessenheitsbeschluss, Standardvertragsklauseln) zulässig.

2 Weisungen des Auftraggebers

2.1 Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers. Der Hauptvertrag und diese Vereinbarung sind die erste Weisung. Weitere Weisungen erteilt der Auftraggeber in Textform (E-Mail genügt) an die in Anlage 4 genannte Ansprechstelle; mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

2.2 Hält der Auftragnehmer eine Weisung für rechtswidrig, teilt er das dem Auftraggeber unverzüglich mit und darf die Weisung bis zur Bestätigung oder Änderung aussetzen.

2.3 Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, werden als Änderungsverlangen behandelt und können gesondert vergütet werden.

2.4 Der Auftragnehmer darf die Daten nur insoweit für eigene Zwecke verarbeiten, als das Unionsrecht oder das Recht eines Mitgliedstaats es verlangt; in diesem Fall informiert er den Auftraggeber vor der Verarbeitung, sofern das Recht dies nicht verbietet.

3 Technische und organisatorische Maßnahmen

3.1 Der Auftragnehmer trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und gewährleistet ein dem Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. Der Auftraggeber hat die Maßnahmen vor Vertragsschluss geprüft und als angemessen anerkannt.

3.2 Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere ersetzen; das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert der Auftragnehmer und stellt die aktuelle Fassung der Anlage 2 auf Anfrage bereit.

3.3 Soweit der Auftraggeber Systeme selbst administriert (zum Beispiel eigene Server, eigener Microsoft-365-Tenant mit eigenen Administratoren), verbleibt die Verantwortung für die dort von ihm gesetzten Konfigurationen und Berechtigungen beim Auftraggeber; Anlage 2 weist das je Leistungsart aus.

4 Vertraulichkeit und Personal

4.1 Der Auftragnehmer setzt nur Beschäftigte und freie Mitarbeitende ein, die auf die Vertraulichkeit verpflichtet und mit den für sie relevanten Datenschutzbestimmungen vertraut gemacht wurden (Art. 28 Abs. 3 Satz 2 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO) und die an den Code of Conduct der Orth & Kellenberger Group gebunden sind.

4.2 Personen mit Zugang zu Daten des Auftraggebers verarbeiten diese nur nach Weisung. Administrative Tätigkeiten erfolgen über persönliche, protokollierte Konten mit Mehrfaktor-Authentifizierung.

5 Unterstützung des Auftraggebers

5.1 Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten nach Art. 12 bis 22 DSGVO (Betroffenenrechte). Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er das Ersuchen unverzüglich an den Auftraggeber weiter und handelt nur nach dessen Weisung.

5.2 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation der Aufsichtsbehörde) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

5.3 Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO erforderlich sind.

5.4 Unterstützungsleistungen, die über den vereinbarten Umfang hinausgehen, vergütet der Auftraggeber nach Aufwand zu den Konditionen des Hauptvertrags, soweit sie nicht durch den Auftragnehmer veranlasst wurden.

6 Meldung von Verletzungen des Schutzes personenbezogener Daten

6.1 Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten, die Daten des Auftraggebers betrifft, unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, an die in Anlage 4 genannte Stelle. Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Datenkategorien und Personen, voraussichtliche Folgen, ergriffene und vorgeschlagene Maßnahmen, Ansprechstelle. Informationen, die noch nicht vorliegen, werden nachgereicht.

6.2 Der Auftragnehmer ergreift unverzüglich die Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und stimmt sie mit dem Auftraggeber ab. Die Meldung an die Aufsichtsbehörde und an betroffene Personen obliegt dem Auftraggeber.

6.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie diesen Auftrag betreffen, und über Ermittlungen in Ordnungswidrigkeits- oder Strafverfahren im Zusammenhang mit der Auftragsverarbeitung.

7 Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat das Recht, die Einhaltung dieser Vereinbarung zu überprüfen – durch Auskünfte, Einsicht in Unterlagen und, nach Anmeldung mit angemessener Frist (in der Regel 14 Tage) und während der üblichen Geschäftszeiten, durch Prüfungen vor Ort beim Auftragnehmer; die Prüfung darf durch einen zur Verschwiegenheit verpflichteten Dritten erfolgen. Betriebsabläufe des Auftragnehmers und Daten anderer Kunden dürfen nicht beeinträchtigt werden.

7.2 Der Nachweis kann auch durch aktuelle Testate, Prüfberichte oder Berichtsauszüge unabhängiger Stellen (Wirtschaftsprüfer, Datenschutz- oder IT-Sicherheitsauditoren, Datenschutzbeauftragter), durch Zertifizierungen nach Art. 42 DSGVO oder genehmigte Verhaltensregeln nach Art. 40 DSGVO erbracht werden. Für Rechenzentren der Unterauftragsverarbeiter genügen deren Zertifikate und Testate.

7.3 Prüfungen, die nicht durch einen konkreten Anlass veranlasst sind, finden höchstens einmal jährlich statt. Der Auftragnehmer kann für die Unterstützung von Prüfungen eine angemessene Vergütung nach Aufwand verlangen.

8 Unterauftragsverarbeiter

8.1 Der Auftraggeber genehmigt die in Anlage 3 genannten Unterauftragsverarbeiter (allgemeine schriftliche Genehmigung, Art. 28 Abs. 2 DSGVO). Welche davon für den konkreten Auftrag eingesetzt werden, ergibt sich aus der gebuchten Leistungsart in Anlage 1.

8.2 Beabsichtigt der Auftragnehmer, einen Unterauftragsverarbeiter hinzuzuziehen oder zu ersetzen, informiert er den Auftraggeber mindestens vier Wochen vorher in Textform. Der Auftraggeber kann innerhalb von zwei Wochen aus wichtigem datenschutzrechtlichen Grund widersprechen. Bei Widerspruch bemühen sich die Parteien um eine Lösung; gelingt sie nicht, kann jede Partei den betroffenen Teil des Hauptvertrags mit einer Frist von vier Wochen kündigen.

8.3 Der Auftragnehmer verpflichtet Unterauftragsverarbeiter durch Vertrag nach Art. 28 Abs. 4 DSGVO auf dieselben Datenschutzpflichten, die ihm selbst obliegen, und prüft sie vor dem Einsatz und regelmäßig. Erfüllt ein Unterauftragsverarbeiter seine Pflichten nicht, haftet der Auftragnehmer dem Auftraggeber gegenüber für dessen Pflichterfüllung.

8.4 Keine Unterauftragsverarbeitung sind Nebenleistungen, die der Auftragnehmer von Dritten bezieht und die sich nicht unmittelbar auf die Hauptleistung beziehen (zum Beispiel Telekommunikation, Post- und Transportdienste, Wartung ohne Datenzugriff, Reinigung, Bewachung, Steuerberatung, Rechtsberatung). Der Auftragnehmer trifft auch hierfür angemessene Vereinbarungen zu Vertraulichkeit und Datenschutz.

9 Datenschutzbeauftragter und Ansprechstellen

9.1 Datenschutz- und Informationssicherheitsbeauftragter des Auftragnehmers ist, extern bestellt, Philip Ladendorf, Datendo XL GmbH, erreichbar über dataprotection@service.orth-kellenberger.com. Ein Wechsel wird dem Auftraggeber mitgeteilt; die aktuellen Kontaktdaten stehen in der Datenschutzerklärung der Websites des Auftragnehmers.

9.2 Sicherheitsvorfälle: security@service.orth-kellenberger.com, rund um die Uhr +49 (0) 8727 969-9855. Weisungen und sonstige Mitteilungen: die in Anlage 4 genannten Personen.

10 Haftung

10.1 Für die Haftung gelten Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags; die dort vereinbarten Haftungsbegrenzungen gelten auch für Ansprüche aus dieser Vereinbarung, soweit zwingendes Recht nicht entgegensteht.

10.2 Der Auftraggeber bleibt für die Rechtmäßigkeit der Verarbeitung, insbesondere für die Rechtsgrundlagen, die Information der betroffenen Personen und die Rechtmäßigkeit seiner Weisungen, verantwortlich (Art. 4 Nr. 7 DSGVO).

11 Rückgabe und Löschung

11.1 Nach Beendigung der Leistungen gibt der Auftragnehmer alle personenbezogenen Daten des Auftraggebers nach dessen Wahl zurück oder löscht sie, einschließlich vorhandener Kopien, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht. Daten in Backups werden im Rahmen des Backup-Zyklus (längstens [90] Tage) überschrieben und bis dahin nicht mehr verarbeitet.

11.2 Zugänge zu Systemen des Auftraggebers werden am Tag der Beendigung entzogen. Dokumentation, die der Auftragnehmer für den Auftraggeber erstellt hat, wird mit der Rückgabe übergeben.

11.3 Der Auftragnehmer bestätigt die Löschung auf Verlangen in Textform. Protokolle über die Löschung bewahrt er nach seinen Aufbewahrungsfristen auf.

12 Schlussbestimmungen

12.1 Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag geht in Datenschutzfragen diese Vereinbarung vor.

12.2 Es gilt deutsches Recht; Gerichtsstand ist der des Hauptvertrags. Sollte eine Bestimmung unwirksam sein, bleibt die Vereinbarung im Übrigen wirksam; an die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung.

12.3 Diese Vereinbarung wird in Textform geschlossen; die elektronische Signatur beider Parteien genügt.

[Ort, Datum] · Auftraggeber: [Name, Funktion] · Auftragnehmer: Orth-Kellenberger Group KG, [Name, Funktion]

Anlage 1 – Gegenstand der Verarbeitung

Zutreffende Leistungsart ankreuzen und ergänzen.

Leistungsart (Marke)	Gegenstand und Zweck	Datenarten	Betroffene
[ ] Managed Services, Projektunterstützung, Second-Level-Support (orandke IT)	Administration, Überwachung und Wartung von Microsoft-365-/Entra-/Intune-Umgebungen, Servern, Netzwerken und Arbeitsplätzen des Auftraggebers; Ticketbearbeitung	Nutzerkonten, Kontakt- und Kommunikationsdaten, Inhalte von Postfächern/Dateien, soweit im Auftrag erforderlich, Geräte- und Protokolldaten, Ticketinhalte	Beschäftigte, Kunden, Lieferanten, Ansprechpartner des Auftraggebers
[ ] Hosting und Cloud (orkenet): Webhosting,	Bereitstellung und Betrieb der gebuchten	alle Daten, die der Auftraggeber auf den	je nach Nutzung durch den

Leistungsart (Marke)	Gegenstand und Zweck	Datenarten	Betroffene
vServer, Dedicated Server, Nextcloud, Domains, E-Mail	Infrastruktur; bei Server-Produkten ohne Zugriff auf Inhalte (Verantwortung Auftraggeber)	Systemen speichert; Domaininhaber- und Kontaktdaten; Protokolldaten	Auftraggeber
[ ] orandke ONE (Business-Portal)	Betrieb einer eigenen Installation mit eigener Datenbank; Updates, Backup-Anbindung, Support	Nutzerkonten, Mitarbeiterstammdaten, Arbeitszeiten und Abwesenheiten, Tickets, E-Mails und Kalender (über Microsoft Graph/IMAP), CRM-Kontakte, Fahrtenbuch, Nachweise, Finanzkennzahlen, Protokolle	Beschäftigte, Kunden, Lieferanten, Ansprechpartner des Auftraggebers
[ ] Standort-/Partnerleistungen (OR-KE)	Leistungen für Endkunden des Partners unter dessen Marke; regionale Systempartner als Unterauftragsverarbeiter	wie Managed Services	Kunden und Beschäftigte des Partners
[ ] Trainings (orandke IT Trainings)	Durchführung von Schulungen, Übungsumgebungen, Teilnahmebescheinigungen	Namen, E-Mail-Adressen, Unternehmen der Teilnehmenden	Beschäftigte des Auftraggebers
[ ] Sonstiges: [Beschreibung]	[Zweck]	[Datenarten]	[Betroffene]

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand des Auftrags, es sei denn, der Auftraggeber weist sie hier aus: [keine / Beschreibung].

Anlage 2 – Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO sind im Dokument „Technische und organisatorische Maßnahmen der Orth-Kellenberger Group KG“ (TOM, Fassung 1.1, Stand 20. Oktober 2026) beschrieben, das Bestandteil dieser Vereinbarung ist. Es unterscheidet nach Leistungsart (interne Systeme des Auftragnehmers, Managed Services in Kundensystemen, Hosting-Produkte, orandke ONE).

Anlage 3 – Unterauftragsverarbeiter

Unterauftragsverarbeiter (Kategorie)	Leistung	Standort	Eingesetzt bei
Hosting- und Rechenzentrumsanbieter mit Sitz in Deutschland	Rechenzentrum, Server, Domainregistrierung	EU (Deutschland, Finnland)	Hosting, orandke ONE, Domains, interne Systeme
Microsoft Ireland Operations Ltd., One Microsoft Place, Dublin 18, Irland	Microsoft 365 (E-Mail, Speicher, Teams), Entra ID, Intune, Defender, Purview; Microsoft Graph für orandke ONE	EU (Rechenzentren Deutschland/EU); Konzernmutter USA – EU-US Data Privacy Framework, Standardvertragsklauseln	Managed Services, orandke ONE, Kommunikation
Anbieter von Konferenz- und Bürodiensten	Büro- und Konferenzdienste für Trainings und Kommunikation	EU; teils Konzernmutter USA – EU-US Data Privacy Framework, Standardvertragsklauseln	Trainings, Kommunikation
Regionale IT-Systempartner (Liste je Partnervertrag)	Vor-Ort-Leistungen unter der Marke OR-KE	Deutschland	OR-KE
Datendo XL GmbH	externer Datenschutz- und Informationssicherheitsbeauftragter (kein Zugriff auf Auftragsdaten im Regelbetrieb)	Deutschland	alle

Veröffentlichungsfassung: Die vollständige Liste mit Firmen und Anschriften erhält der Auftraggeber mit dem Vertrag und auf Anfrage; Änderungen werden nach Ziffer 8.2 angekündigt. Stand 23. Oktober 2026.

Anlage 4 – Weisungsberechtigte und Ansprechstellen

Rolle	Auftraggeber	Auftragnehmer
Weisungsberechtigt	[Name, Funktion, E-Mail, Telefon]	–
Weisungsempfänger / Ansprechstelle Auftrag	–	[Name, Funktion], support@mail.orandke-it.com, +49 (0) 8727 969-9855
Datenschutzbeauftragter	[Name, E-Mail]	Philip Ladendorf, Datendo XL GmbH, dataprotection@service.orth-kellenberger.com
Sicherheitsvorfälle (24 h)	[Name, E-Mail, Telefon]	security@service.orth-kellenberger.com, +49 (0) 8727 969-9855