orth & kellenberger GROUP

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO · Orth-Kellenberger Group KG und alle Marken · Fassung 1.1 · Stand 2. November 2026 · Anlage 2 zur Vereinbarung über Auftragsverarbeitung

Dieses Dokument beschreibt die Maßnahmen, mit denen die Orth-Kellenberger Group KG personenbezogene Daten schützt – eigene und die ihrer Kunden. Es ersetzt die Anlage 2 der Orth & Cie. KG vom Januar 2024. Wo die Verantwortung je nach Leistungsart beim Kunden liegt, ist das ausgewiesen. Verantwortlich: die Geschäftsführung; Sicherheitsverantwortlicher: Jedidjah Orth (security@service.orth-kellenberger.com); Datenschutz- und Informationssicherheitsbeauftragter (extern): Philip Ladendorf, Datendo XL GmbH (dataprotection@service.orth-kellenberger.com).

1 Geltung und Leistungsarten

Die Maßnahmen gelten für alle Gesellschaften und Marken der Orth & Kellenberger Group und werden nach vier Leistungsarten unterschieden:

Kürzel	Leistungsart	Wer verantwortet was
A	Interne Systeme des Auftragnehmers (Microsoft 365, orandke ONE der Gruppe, Büro, Endgeräte)	vollständig Orth-Kellenberger Group KG
B	Managed Services, Projektunterstützung, Support in Kundensystemen (Microsoft 365, Server, Netzwerke des Kunden)	Kunde ist Verantwortlicher und Eigentümer der Systeme; Orth-Kellenberger Group KG verantwortet ihr Handeln, ihre Zugänge und Geräte; Konfigurationen folgen dem Auftrag
C	Hosting-Produkte (orkenet): Webhosting, vServer, Dedicated Server, Nextcloud, Domains, E-Mail	Infrastruktur und Verwaltungssysteme: Orth-Kellenberger Group KG mit Rechenzentrumspartnern; Inhalte und Serverkonfiguration bei Server-Produkten: Kunde
D	orandke ONE (Business-Portal, eine Installation je Kunde)	Betrieb, Updates, Plattformsicherheit: Orth-Kellenberger Group KG; Nutzer, Rechte und

Kürzel	Leistungsart	Wer verantwortet was
		Inhalte: Kunde

2 Organisation und Verantwortung

- Datenschutz- und Informationssicherheitsbeauftragter extern bestellt (Datendo XL GmbH), beim BayLDA gemeldet; interner Sicherheitsverantwortlicher und Compliance-Beauftragter in der Geschäftsführung; Berichtslinie an Geschäftsführung und Verwaltungsrat.
- Code of Conduct der Gruppe mit eigenem Kapitel Datenschutz und Informationssicherheit, verbindlich für Mitarbeitende, freie Trainer, Standortpartner und Lieferanten (Vertragsbestandteil).
- Verpflichtung aller Beschäftigten und freien Mitarbeitenden auf Vertraulichkeit (Art. 29, 32 Abs. 4 DSGVO) vor Aufnahme der Tätigkeit; jährliche Schulung; Unterweisung zu Phishing und Social Engineering.
- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO), Löschkonzept mit Fristen je Datenart, Prozess für Betroffenenanfragen (Auskunft innerhalb eines Monats), Prozess für Datenschutzverletzungen (interne Meldung sofort, Bewertung durch den Datenschutzbeauftragten, Meldung an die Aufsicht innerhalb von 72 Stunden).
- Auftragsverarbeiter werden vor Einsatz geprüft (Vertrag nach Art. 28, Standort, Zertifikate) und in einer Liste geführt; Unterauftragsverarbeiter nur aus der genehmigten Liste.
- Regelmäßige Überprüfung dieser Maßnahmen: jährlich durch den Datenschutz- und Informationssicherheitsbeauftragten, anlassbezogen nach Vorfällen oder Systemänderungen; orandke ONE zusätzlich durch externe Sicherheitsprüfungen (zuletzt zwei Prüfungen im September 2026).

3 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Zutrittskontrolle

- Rechenzentren der Hosting-Partner (Standorte in der EU: Deutschland und Finnland): elektronische Zutrittskontrolle mit Protokollierung, Sicherheitszaun, Videoüberwachung an Ein- und Ausgängen und Serverräumen, 24/7-Besetzung, Besucher nur in Begleitung, dokumentierte Schlüsselvergabe; Nachweis durch Zertifikate und Testate der Betreiber (ISO 27001).

- Zentrale Falkenberg und Standorte: abschließbare Büroräume, Schlüssel- und Zutrittsregelung, Besucher nur in Begleitung; Serverschränke verschlossen; keine Kundendaten in Papierform außerhalb verschlossener Schränke; Clean-Desk-Regel.
- Eigene Hardware in Rechenzentren (Colocation) nur im eigenen, verschlossenen Rack.

3.2 Zugangskontrolle (Systeme)

- Alle Konten persönlich; **Mehrfaktor-Authentifizierung ist Pflicht** für alle Nutzer- und Administratorkonten (Microsoft Entra ID mit Conditional Access: Zugriff nur von konformen, verwalteten Geräten und nach Risikobewertung; TOTP bei lokalen Konten in orandke ONE und auf Service-Systemen).
- **Getrennte Administratorkonten:** Nutzer haben auf ihren Geräten keine lokalen Administratorrechte; administrative Tätigkeiten – in eigenen wie in Kundensystemen – nur über eigene Admin-Konten je Person, nie über das Alltagskonto; privilegierte Rechte zeitlich begrenzt, wo die Umgebung es erlaubt (Privileged Identity Management).
- Passwortrichtlinie (Mindestlänge, keine Wiederverwendung), zentraler Passwort-Manager; Zugangsdaten nie in Dokumenten, E-Mails oder Chats; Bruteforce-Schutz und Sperrung nach Fehlversuchen.
- Endgeräte: ausschließlich firmeneigene Geräte, verwaltet über Microsoft Intune (Compliance-Richtlinien, Verschlüsselung mit BitLocker/FileVault, automatische Sperre, Fernlöschung), Microsoft Defender auf jedem Endgerät (Virenschutz, EDR), aktuelle Patchstände erzwungen.
- Entzug von Zugängen am Tag des Ausscheidens oder Auftragsendes – in eigenen und in Kundensystemen; geführter Austrittsprozess in orandke ONE (Konto sperren, Zuständigkeiten übertragen, Protokoll).
- Leistungsart C (Server-Produkte): Server-Passwörter vergibt der Kunde nach erstmaliger Inbetriebnahme selbst; sie sind dem Auftragnehmer nicht bekannt; Verwaltungsoberfläche (Plesk) mit Passwortrichtlinie und Zwei-Faktor-Option; Zugang zu Webhosting-Systemen nur für berechtigte Administratoren des Auftragnehmers.
- Leistungsart D (orandke ONE): Jede Installation ist nur über die zentrale Anmeldung app.orandke.one erreichbar (Router mit gemeinsamem Geheimnis, direkter Zugriff gesperrt, dokumentierter Notfallzugang mit Schlüssel, Versuchsbremse und Protokoll); Anmeldung mit Microsoft Entra ID oder lokalem Konto mit Passwortrichtlinie (12 Zeichen) und TOTP-Zwei-Faktor (für Administratoren erzwingbar); Sitzungen nur als Hash gespeichert, HttpOnly-Cookies; Geräteübersicht je Nutzer.

3.3 Zugriffskontrolle (Berechtigungen)

- Rollen- und Rechtekonzept nach dem Prinzip der geringsten Rechte; Vergabe dokumentiert über ein verbindliches Berechtigungsverfahren; regelmäßige Überprüfung der Berechtigungen (mindestens jährlich, bei Rollenwechsel sofort).
- Leistungsart B: Zugriff auf Kundensysteme nur im Umfang des Auftrags; kein Lesen von Postfächern, Dateien oder Chats von Kundenmitarbeitenden ohne schriftliche Freigabe des Kunden; bei Microsoft-365-Anbindungen Begrenzung der App-Berechtigungen (Exchange Application Access Policy) auf freigegebene Postfächer; Bestandskunden mit nur einem gemeinsamen globalen Administratorkonto erhalten eine dokumentierte Empfehlung zur Umstellung.
- Leistungsart D: Rollen Administrator, lokaler Administrator, Mitarbeiter sowie Rechte (Finanzen, Personal, CRM, Schulungen, Globaler Leser), direkt oder über Gruppen vererbt; jede Anfrage wird serverseitig geprüft; Sichtbarkeit je Gesellschaft (Kunden, Tickets, Zeiten); Rechte-Matrix aus dem Programmcode erzeugt und dokumentiert.
- Microsoft Purview: Vertraulichkeitskennzeichnung von Dokumenten und E-Mails, Richtlinien gegen Datenabfluss (DLP) für Kundendaten, Aufbewahrungsrichtlinien.

3.4 Trennungskontrolle

- Daten verschiedener Kunden werden logisch, bei orandke ONE physisch getrennt verarbeitet: **eine Installation und eine Datenbank je Kunde**; Mandanten innerhalb der Gruppe mit Sichtbarkeit je Gesellschaft.
- Hosting: getrennte Kundenbereiche je Vertrag (Plesk-Abonnements, eigene Datenbanken, eigene Systemnutzer); Backups auf logisch oder physisch getrennten Systemen.
- Produktiv-, Test- und Schulungsumgebungen sind getrennt; Übungs-Tenants und Laborumgebungen enthalten nur Testdaten und werden nach dem Seminar gelöscht.
- Interne Daten der Gruppe und Kundendaten werden in getrennten Bereichen (SharePoint-Sites, Tenants, Mandanten) geführt.

3.5 Pseudonymisierung und Verschlüsselung

- Transportverschlüsselung (TLS 1.2/1.3) für alle Websites, Portale, E-Mail-Verbindungen und Fernzugriffe; Zertifikate automatisiert (Let's Encrypt) oder durch die Rechenzentrumspartner.
- Verschlüsselung ruhender Daten: Endgeräte vollständig verschlüsselt; Microsoft 365 verschlüsselt ruhend; orandke ONE verschlüsselt Geheimnisse in der Datenbank (Master-Key

außerhalb der Datenbank) und Backups mit libsodium, der private Schlüssel liegt ausschließlich beim Kunden; Hosting-Backups verschlüsselt.

- Pseudonymisierung, soweit der Zweck es erlaubt (zum Beispiel Testdaten, Übungskonten nach Schema teilnehmer01@…); bei Server-Produkten (C) obliegt die Pseudonymisierung dem Kunden.

4 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Weitergabekontrolle

- Übertragung personenbezogener Daten nur verschlüsselt (TLS, SFTP, verschlüsselte Archive mit getrenntem Schlüsselversand); keine Kundendaten auf privaten Geräten, privaten Cloud-Speichern, USB-Sticks oder Messengern; Purview-DLP blockiert den Versand gekennzeichneter Daten an externe Empfänger ohne Freigabe.
- Firmendaten ausschließlich in den Unternehmens-Cloudspeichern (Microsoft 365; Google Workspace für freie Trainer und die Organisation e.V.).
- Datenträger: Festplatten der Rechenzentrumspartner werden nach Kündigung mehrfach überschrieben oder im Rechenzentrum zerstört; eigene Datenträger werden vor Weitergabe oder Entsorgung zertifiziert gelöscht oder physisch vernichtet; Kundengeräte zur Reparatur oder Entsorgung nur mit dokumentierter Löschung.
- Fernwartung nur über protokollierte, verschlüsselte Verbindungen mit persönlichen Konten; Sitzungen werden im Ticket dokumentiert.

4.2 Eingabekontrolle

- Protokollierung von Anlage, Änderung und Löschung personenbezogener Daten in allen Systemen des Auftragnehmers: orandke ONE führt ein automatisches Aktivitätsprotokoll jeder schreibenden Aktion (wer, was, wann, womit) mit 365 Tagen Aufbewahrung und CSV-Export; Microsoft 365 Audit-Log; Server-Logs mit 14 Tagen.
- Änderungen an Kundensystemen folgen dem Änderungsprozess: Ticket, Freigabe, Wartungsfenster, Dokumentation, Rückfallplan.
- Bei Server-Produkten (C) gibt der Kunde die Daten selbst ein; die Eingabekontrolle obliegt ihm.

5 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

5.1 Verfügbarkeitskontrolle

- Rechenzentren: unterbrechungsfreie Stromversorgung, Netzersatzanlagen, Klimatisierung, Brandschutz, redundante Netzanbindung, dauerhaft aktiver DDoS-Schutz und Firewalls der Betreiber (Hosting- und Rechenzentrumsanbieter mit Sitz in Deutschland; Namen in Anlage 3 der jeweiligen Vereinbarung).
- Server und Hosting: Festplattenspiegelung, Monitoring aller relevanten Systeme mit Alarmierung, Software-Firewall und Portbeschränkungen, regelmäßige Sicherheitsupdates nach dem Stand der Technik; Websites zusätzlich mit Wordfence (Angriffserkennung, Sperrung).
- Backups: tägliche Sicherung aller relevanten internen Systeme mit Aufbewahrung nach Backup-Zyklus; Hosting-Backups je gebuchtem Leistungsumfang; orandke ONE täglich verschlüsselt in den Cloud-Speicher des Kunden (OneDrive/Google Drive); Microsoft 365 durch Microsoft-Redundanz und zusätzliche Sicherung nach Aufbewahrungsrichtlinie; bei Server-Produkten (C) obliegt die Datensicherung dem Kunden.
- Endgeräteschutz: Microsoft Defender mit Echtzeitschutz, Spam- und Phishing-Filter in Microsoft 365, Schutz vor Schadsoftware in Anhängen (Safe Attachments/Links).
- Updates für orandke ONE sind signiert (Ed25519, privater Schlüssel offline beim Anbieter); die Installation prüft Signatur, Version und Prüfsumme, sichert Dateien und Datenbank, spielt ein, prüft sich selbst und rollt bei Fehlern automatisch zurück; Update-Kanäle und Wartungsfenster je Kunde.

5.2 Rasche Wiederherstellbarkeit

- Backup- und Wiederherstellungskonzept mit definierter Eskalationskette (wer wird wann informiert); Wiederherstellung wird mindestens jährlich geprobt und dokumentiert.
- Notfallplan für Ausfall des Rechenzentrums, des Microsoft-365-Tenants und von orandke ONE (Router-Notfallzugang, Einzelinstallation ohne Router möglich).
- Redundante Kommunikationswege (Telefonie über Microsoft Teams und Cloud-Telefonanlage).

6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 DSGVO)

- Datenschutz-Management: Verzeichnis der Verarbeitungstätigkeiten, Löschkonzept, Richtlinien (IT-Sicherheit, Datenschutz, Geräte- und Cloud-Nutzung, KI-Werkzeuge), jährliche Überprüfung

durch den Datenschutz- und Informationssicherheitsbeauftragten, Bericht an die Geschäftsführung.

- Vorfallmanagement: Meldeweg security@service.orth-kellenberger.com rund um die Uhr; Bewertung, Eindämmung, Beweissicherung, Information betroffener Kunden ohne Verzögerung; Nachbereitung mit Maßnahmenliste.
- Auftragskontrolle: Verarbeitung nur nach dokumentierter Weisung; Auswahl und Prüfung von Unterauftragsverarbeitern; AV-Verträge mit allen Dienstleistern; Liste der Unterauftragsverarbeiter wird gepflegt.
- Datenschutz durch Technikgestaltung und Voreinstellungen: Neue Systeme und Projekte werden vor Einführung auf Datenschutz und Sicherheit geprüft (Datenschutz-Folgenabschätzung bei hohem Risiko); datensparsame Voreinstellungen (zum Beispiel keine Website-Tracker, Formulardaten nur per E-Mail, Karten erst nach Klick).
- Prüfungen: orandke ONE mit automatisiertem Prüflauf aller Funktionen in allen Rollen vor jedem Release und externen Sicherheitsprüfungen; Websites und Server mit regelmäßigen Schwachstellenprüfungen; Berechtigungs- und Zugangsreview mindestens jährlich.
- Schulung und Sensibilisierung: jährliche Datenschutz- und Sicherheitsschulung, Phishing-Übungen, Unterweisung neuer Mitarbeitender vor Zugang zu Kundendaten.

7 Besondere Regelungen für Leistungsart B (Kundensysteme)

- Der Kunde bleibt Verantwortlicher; der Auftragnehmer arbeitet in den Systemen des Kunden nach dessen Konfiguration und Weisung.
- Der Auftragnehmer verwendet in Kundensystemen ausschließlich persönliche Administratorkonten mit Mehrfaktor-Authentifizierung, protokolliert seine Tätigkeiten im Ticket und entzieht Zugänge mit Auftragsende.
- Empfehlungen des Auftragnehmers zur Härtung der Kundenumgebung (persönliche Admin-Konten, zeitlich begrenzte Rechte, Conditional Access, Backup) werden dokumentiert; setzt der Kunde sie nicht um, liegt das Risiko beim Kunden.
- Der Auftragnehmer legt keine Konten, Weiterleitungen oder Zugänge an, die der Kunde nicht kennt.

8 Änderungen

Dieses Dokument wird bei wesentlichen Änderungen der Systeme oder Prozesse, mindestens jährlich, überprüft. Die jeweils gültige Fassung erhalten Kunden auf Anfrage; sie ersetzt frühere Fassungen, ohne das vereinbarte Schutzniveau zu unterschreiten.