Vereinbarung zur Auftragsdatenbearbeitung (ADV)

Seamlesswork AG | Letzte Aktualisierung: Juli 2026

Dieser Vereinbarung zur Auftragsdatenbearbeitung ("ADV") ist integraler Bestandteil der Allgemeinen Geschäftsbedingungen ("AGB") für Seamless und regelt die Verarbeitung Personenbezogener Daten durch die Seamlesswork AG im Auftrag des Kunden im Zusammenhang mit dem Seamless-Produkt. Mit der Annahme der AGB akzeptiert der Kunde auch diesen ADV.

Inhalt

1. Zweck

1.1 Die Seamlesswork AG ("Anbieter") stellt Kunden Seamless, eine Governance-Lösung für Microsoft 365 ("Produkt"), zur Verfügung. Das Produkt wird gemäss den AGB bereitgestellt.

1.2 Die Bereitstellung des Produkts umfasst die Verarbeitung Personenbezogener Daten durch den Anbieter im Auftrag des Kunden. Zweck dieses ADV ist es, die Rechte und Pflichten der Parteien im Zusammenhang mit dieser Verarbeitung in Übereinstimmung mit dem anwendbaren Datenschutzrecht festzulegen.

1.3 Dieser ADV soll die Parteien bei der Einhaltung der EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, "DSGVO") und des revidierten Schweizer Bundesgesetzes über den Datenschutz ("revDSG", SR 235.1) sowie weiterer anwendbarer Datenschutzgesetze unterstützen.

2. Anwendungsbereich

2.1 Dieser ADV gilt für sämtliche Tätigkeiten unter den AGB, bei denen der Anbieter Personenbezogene Daten im Auftrag des Kunden verarbeitet. Die Kategorien der verarbeiteten Personenbezogenen Daten, die Verarbeitungszwecke, die Kategorien betroffener Personen und die anwendbaren Aufbewahrungsfristen sind in Anhang 1 zu diesem ADV festgelegt.

2.2 Der Anbieter verarbeitet ausschliesslich die zur Bereitstellung des Produkts unbedingt erforderlichen Personenbezogenen Daten. Der Anbieter verarbeitet keine Endbenutzer-Inhalte (Dokumente, Dateien, Nachrichten oder sonstige Kommunikation), die durch Benutzer des Kunden in Microsoft 365 erstellt oder gespeichert werden. Solche Inhalte verbleiben ausschliesslich im Microsoft-365-Tenant des Kunden und sind für den Anbieter nicht zugänglich.

3. Definitionen

3.1 Sofern in diesem ADV nicht anders definiert, haben alle Begriffe die ihnen in der DSGVO, im revDSG oder in den AGB zugewiesene Bedeutung.

Begriff	Definition
Verantwortlicher	Der Kunde als natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung Personenbezogener Daten entscheidet.
Auftragsverarbeiter	Der Anbieter (Seamlesswork AG), der Personenbezogene Daten im Auftrag des Kunden gemäss diesem ADV und den AGB verarbeitet.
Unterauftragsverarbeiter	Jeder vom Anbieter beauftragte Drittanbieter, der Personenbezogene Daten im Zusammenhang mit dem Produkt verarbeitet. Eine Liste der derzeit eingesetzten Unterauftragsverarbeiter findet sich in Anhang 3 zu diesem ADV.

Begriff	Definition
Sicherheitsvorfall	Jede Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmässigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder zum unbefugten Zugang zu Personenbezogenen Daten führt, die nach diesem ADV verarbeitet werden.
Betroffene Person	Jede identifizierte oder identifizierbare natürliche Person, deren Personenbezogene Daten nach diesem ADV verarbeitet werden.
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten.
revDSG	Das revidierte Schweizer Bundesgesetz über den Datenschutz, SR 235.1, in Kraft seit 1. September 2023.
Data Act	Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung.
Nicht-personenbezogene Daten	Alle Daten, die nach dem anwendbaren Datenschutzrecht nicht als Personenbezogene Daten gelten.
Mixed Dataset	Ein Datensatz, der sowohl Personenbezogene Daten als auch Nicht-personenbezogene Daten enthält.
Exportierbare Daten	Kunden-bezogene Daten (personenbezogen oder nicht-personenbezogen), die innerhalb der Produktumgebung erzeugt oder gespeichert werden und die der Anbieter dem Kunden oder einem vom Kunden bestimmten Dritten gemäss dem Data Act und diesem ADV zur Verfügung stellen muss. Daten, die ausschliesslich in Microsoft 365, Entra ID oder anderen vom Kunden vollständig kontrollierten Systemen verbleiben, sind ausgenommen.

Begriff	Definition
Switching	Die Migration Exportierbarer Daten durch den Kunden vom Produkt zu einem anderen Datenverarbeitungsdienst oder in die eigene Umgebung des Kunden gemäss dem Data Act und diesem ADV.

4. Rollen und rechtliche Verantwortung

4.1 Im Rahmen dieses ADV handelt der Kunde als Verantwortlicher und der Anbieter als Auftragsverarbeiter im Sinne der DSGVO und des revDSG. Der Kunde bleibt allein verantwortlich für die Rechtmässigkeit der von ihm angewiesenen Verarbeitung Personenbezogener Daten.

4.2 Der Anbieter verarbeitet Personenbezogene Daten nur im Auftrag und auf dokumentierte Weisung des Kunden gemäss diesem ADV und den AGB, sofern er nicht durch das anwendbare Recht zu einer anderen Verarbeitung verpflichtet ist. In einem solchen Fall informiert der Anbieter den Kunden vor der Verarbeitung über die rechtliche Anforderung, sofern dies nicht gesetzlich verboten ist.

4.3 Der Kunde sichert zu, dass die Übermittlung Personenbezogener Daten an den Anbieter und die in diesem ADV beschriebene Verarbeitung nach anwendbarem Datenschutzrecht zulässig sind. Der Kunde ist für die Erfüllung seiner eigenen Pflichten als Verantwortlicher verantwortlich, einschliesslich der Bereitstellung erforderlicher Informationen an betroffene Personen und der Einholung notwendiger Einwilligungen.

4.4 Der Anbieter stellt dem Kunden die in Anhang 2 zu diesem ADV beschriebenen technischen und organisatorischen Massnahmen zur Verfügung. Der Kunde ist verantwortlich für die Beurteilung, ob diese Massnahmen für seine vorgesehene Nutzung des Produkts und die zu verarbeitenden Personenbezogenen Daten ausreichend sind.

4.5 Der Kunde informiert den Anbieter unverzüglich, wenn ihm eine Verletzung von Datenschutzbestimmungen oder eine Anweisung bekannt wird, die nach Auffassung des Kunden gegen anwendbares Datenschutzrecht verstösst.

4.6 Auf Anfrage stellt der Kunde dem Anbieter alle Informationen zur Verfügung, die zur Führung eines Verzeichnisses sämtlicher im Auftrag des Kunden ausgeführter Verarbeitungstätigkeiten erforderlich sind, soweit der Anbieter diese Informationen nicht anderweitig zur Verfügung hat.

4.7 Sofern der Anbieter im Zusammenhang mit der Verarbeitung Personenbezogener Daten unter diesem ADV einer Behörde oder anderen Stelle Auskünfte erteilen oder mit solchen Stellen kooperieren muss, unterstützt der Kunde den Anbieter auf erste Anforderung bei der Bereitstellung dieser Auskünfte und der Erfüllung etwaiger Mitwirkungspflichten.

5. Datenverarbeitung und Weisungsgebundenheit

5.1 Der Anbieter verarbeitet Personenbezogene Daten ausschliesslich gemäss den dokumentierten Weisungen des Kunden, wie sie in diesem ADV festgelegt sind, sofern nicht das anwendbare Recht etwas anderes vorschreibt. Die Weisungen des Kunden sind grundsätzlich abschliessend in diesem

ADV festgelegt. Einzelweisungen, die von diesem ADV abweichen oder über ihn hinausgehende Anforderungen stellen, bedürfen der vorgängigen schriftlichen Zustimmung des Anbieters und können zusätzliche, vom Kunden zu tragende Kosten verursachen.

5.2 Der Anbieter stellt sicher, dass alle Personen, die zur Verarbeitung Personenbezogener Daten im Auftrag des Kunden befugt sind, zur Vertraulichkeit verpflichtet sind, sei es vertraglich oder gesetzlich.

5.3 Der Anbieter verarbeitet Personenbezogene Daten innerhalb des Europäischen Wirtschaftsraums (EWR) oder der Schweiz. Eine Übermittlung Personenbezogener Daten in ein Land ausserhalb des EWR oder der Schweiz erfolgt nur, wenn die Anforderungen von Kapitel V DSGVO und der anwendbaren Bestimmungen des revDSG erfüllt sind und der Kunde vorab informiert wird.

5.4 Der Anbieter darf Personenbezogene Daten so anonymisieren oder aggregieren, dass eine Identifikation einzelner betroffener Personen unmöglich ist, und solche anonymisierten oder aggregierten Daten zur Verbesserung der Sicherheit und Qualität des Produkts verwenden. Der Anbieter darf solche Daten nicht zum Training von KI-Modellen verwenden, ohne dass der Kunde vorab schriftlich zugestimmt hat (siehe Abschnitt 7.2.1 der AGB). Anonymisierte Daten gelten im Sinne dieses ADV nicht als Personenbezogene Daten.

6. Technische und organisatorische Massnahmen

6.1 Der Anbieter implementiert geeignete technische und organisatorische Massnahmen ("TOMs"), um ein dem Risiko angemessenes Sicherheitsniveau gemäss Art. 32 DSGVO und Art. 8 revDSG zu gewährleisten. Die derzeit umgesetzten TOMs sind in Anhang 2 zu diesem ADV beschrieben. Der Anbieter ist berechtigt, die TOMs im Laufe der Zeit anzupassen, sofern das Gesamtschutzniveau nicht reduziert wird.

6.2 Der Anbieter stellt sicher, dass alle Personen, die mit der Verarbeitung Personenbezogener Daten im Auftrag des Kunden betraut sind, einer angemessenen Vertraulichkeitspflicht unterliegen.

7. Unterstützung, Information und Kooperation

7.1 Der Anbieter unterstützt den Kunden, soweit technisch machbar und rechtlich erforderlich, bei der Erfüllung seiner Pflichten aus DSGVO und revDSG, einschliesslich Betroffenenrechten, Meldung von Datenschutzverletzungen, Sicherheitspflichten und Datenschutz-Folgenabschätzungen. Der Kunde erstattet dem Anbieter die für solche Unterstützung dokumentiert entstandenen Kosten, sofern der Bedarf nicht aus einer Pflichtverletzung des Anbieters resultiert.

7.2 Wendet sich eine betroffene Person mit der Ausübung ihrer Rechte direkt an den Anbieter, leitet der Anbieter die Anfrage ohne unangemessene Verzögerung an den Kunden weiter. Der Anbieter beantwortet solche Anfragen nicht unmittelbar, sofern dies nicht gesetzlich vorgeschrieben ist oder der Kunde dazu vorab ermächtigt hat.

7.3 Der Anbieter stellt dem Kunden alle Informationen zur Verfügung, die vernünftigerweise erforderlich sind, um die Einhaltung der in diesem ADV festgelegten Pflichten nachzuweisen.

7.4 Der Kunde hat das Recht, die Einhaltung dieses ADV durch den Anbieter mit einer Vorankündigung von mindestens dreissig (30) Tagen schriftlich auf eigene Kosten zu auditieren. Der

Anbieter kann nach eigenem Ermessen einen entsprechenden Nachweis durch einen aktuellen Auditbericht oder eine relevante Zertifizierung (z.B. ISO 27001) erbringen. Hat der Kunde begründeten Anlass zur Annahme, dass eine solche Dokumentation nicht ausreichend ist, kann er eine Vor-Ort-Inspektion verlangen. Stellt das Audit eine wesentliche Pflichtverletzung des Anbieters fest, so trägt der Anbieter die angemessenen Kosten des Audits.

7.5 Sobald der Anbieter Kenntnis von einem Sicherheitsvorfall erlangt, informiert er den Kunden unverzüglich und stellt verfügbare Informationen über Art, Umfang und voraussichtliche Folgen des Vorfalls sowie die getroffenen Massnahmen zur Verfügung.

8. Unterauftragsverarbeiter

8.1 Der Kunde erteilt dem Anbieter eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern für die Verarbeitung Personenbezogener Daten unter diesem ADV. Eine Liste der derzeit vom Anbieter eingesetzten Unterauftragsverarbeiter findet sich in Anhang 3 zu diesem ADV und wird von Zeit zu Zeit aktualisiert.

8.2 Der Anbieter informiert den Kunden vorab über jede beabsichtigte Änderung der Liste der Unterauftragsverarbeiter, einschliesslich der Beauftragung neuer oder des Austauschs bestehender Unterauftragsverarbeiter. Der Kunde kann einer solchen Änderung innerhalb von dreissig (30) Tagen nach Mitteilung aus angemessenen Datenschutzgründen widersprechen. Erhebt der Kunde einen begründeten Widerspruch und kann der Anbieter dem nicht entsprechen, kann jede Partei die AGB gemäss deren Bestimmungen kündigen.

8.3 Der Anbieter erlegt allen Unterauftragsverarbeitern in einem schriftlichen Vertrag mindestens gleichwertige Datenschutzpflichten auf, wie sie in diesem ADV festgelegt sind. Der Anbieter haftet dem Kunden gegenüber für die Erfüllung der Pflichten der Unterauftragsverarbeiter unter diesem ADV in dem Umfang, in dem er auch selbst haften würde.

8.4 Befindet sich ein Unterauftragsverarbeiter ausserhalb der Schweiz oder des EWR, stellt der Anbieter sicher, dass ein geeigneter Datenübermittlungsmechanismus besteht, einschliesslich, soweit anwendbar, der Standardvertragsklauseln der EU (Durchführungsbeschluss (EU) 2021/914) und der vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) anerkannten Schweizer Standardvertragsklauseln (Swiss SCCs) oder gleichwertiger Schutzmassnahmen nach revDSG.

9. Laufzeit und Beendigung

9.1 Dieser ADV tritt mit denselben Datum in Kraft wie die AGB und bleibt in Kraft, solange der Anbieter Personenbezogene Daten im Auftrag des Kunden gemäss den AGB verarbeitet.

9.2 Mit Beendigung der AGB aus jeglichem Grund wird der Anbieter nach Wahl des Kunden und innerhalb angemessener Frist: (a) sämtliche unter diesem ADV verarbeiteten Personenbezogenen Daten an den Kunden in einem strukturierten, gängigen und maschinenlesbaren Format zurückgeben; oder (b) alle solchen Personenbezogenen Daten sicher löschen oder vernichten und dies schriftlich bestätigen. Der Kunde kann seine Seamless-Konfigurationsdaten jederzeit über das Seamless Admin Center dauerhaft löschen; eine solche Löschung ist unwiderruflich.

9.3 Der Anbieter darf Personenbezogene Daten über den in Abschnitt 9.2 genannten Zeitraum hinaus aufbewahren, soweit dies nach anwendbarem Recht erforderlich ist oder zur Geltend-

machung, Ausübung oder Verteidigung von Rechtsansprüchen notwendig. Solche aufbewahrten Daten unterliegen weiterhin den Vertraulichkeits- und Sicherheitsverpflichtungen dieses ADV.

10. Haftung und Freistellung

10.1 Die Haftung des Anbieters unter diesem ADV richtet sich nach den Beschränkungen und Haftungsausschlüssen der AGB (Kapitel 11). Soweit das anwendbare Datenschutzrecht (insbesondere Art. 82 DSGVO) eine Beschränkung nicht zulässt, wird die Haftung des Anbieters durch diesen ADV nicht begrenzt.

10.2 Macht ein Dritter gegenüber dem Anbieter Ansprüche geltend, die aus einer Verletzung dieses ADV durch den Kunden, einer Verletzung des anwendbaren Datenschutzrechts durch den Kunden oder den Weisungen des Kunden an den Anbieter resultieren, stellt der Kunde den Anbieter von diesen Ansprüchen einschliesslich angemessener Anwaltskosten frei.

10.3 Der Kunde stellt den Anbieter von administrativen Bussgeldern oder Strafen frei, die einer Aufsichtsbehörde gegenüber dem Anbieter verhängt werden, soweit diese auf das Verhalten oder die Weisungen des Kunden zurückzuführen sind.

11. Bestimmungen zum Data Act

11.1 Soweit anwendbar erkennen die Parteien an, dass der Anbieter im Verhältnis zu Exportierbaren Daten innerhalb der Produktumgebung als Anbieter von Datenverarbeitungsdiensten und/oder als Datenhalter im Sinne des Data Act gelten kann. Daten, die ausschliesslich in Microsoft 365, Entra ID oder anderen vom Kunden kontrollierten Systemen verbleiben, fallen nicht unter diesen Abschnitt 11.

11.2 Der Anbieter stellt dem Kunden Exportierbare Daten in einem gängigen, maschinenlesbaren und strukturierten Format über Self-Service-Schnittstellen zur Verfügung, einschliesslich der Export-Funktionalitäten des Seamless Admin Center und der Seamless API. Standard-Exporte sind kostenfrei. Über die Standard-Exportfunktionalität hinausgehende Aufwände, die ausdrücklich vom Kunden angefordert werden, können zum Standard-Stundensatz des Anbieters berechnet werden.

11.3 Der Anbieter stellt keine ungerechtfertigten vertraglichen, technischen oder kommerziellen Hindernisse für das Switching auf. Insbesondere: (a) erhebt der Anbieter keine spezifischen Switching-Gebühren, ausser für ausdrücklich vom Kunden angeforderte zusätzliche Leistungen, die über die Standard-Export-Funktionalität hinausgehen; (b) ermöglicht der Anbieter, soweit technisch machbar, den parallelen Betrieb des Produkts mit einem anderen Dienst während eines angemessenen Übergangszeitraums; und (c) leistet der Anbieter angemessene Zusammenarbeit und stellt Informationen zur Verfügung, die für eine effektive Migration Exportierbarer Daten an einen anderen Dienst oder in die eigene Umgebung des Kunden notwendig sind.

11.4 Der Anbieter stellt dem Kunden Dokumentation zu den Exportformaten, relevanten Datenstrukturen und Schnittstellen einschliesslich APIs zur Verfügung, die für den Zugriff auf Exportierbare Daten innerhalb des Produkts genutzt werden. Diese Dokumentation ist verfügbar unter https://sml-api.io/docs/ oder auf Anfrage beim Anbieter.

11.5 Erhält der Anbieter eine rechtsverbindliche Aufforderung einer Behörde aus einem Drittland zum Zugriff auf Nicht-personenbezogene Daten oder Mixed Datasets, die unter den Data Act

fallen und im EWR oder der Schweiz gespeichert sind, wird der Anbieter, soweit gesetzlich zulässig: (a) den Kunden unverzüglich über die Aufforderung informieren; (b) die Rechtmässigkeit und den Umfang der Aufforderung prüfen und offensichtlich rechtswidrige Aufforderungen anfechten; (c) Zugriff nur in dem Umfang gewähren, der zur Erfüllung strikt erforderlich ist; und (d) Aufforderung und Reaktion angemessen dokumentieren.

12. Anwendbares Recht und Gerichtsstand

12.1 Dieser ADV unterliegt dem Schweizer Recht unter Ausschluss seiner Kollisionsnormen sowie unter Ausschluss des UN-Übereinkommens über Verträge über den internationalen Warenkauf (CISG). Soweit die DSGVO Anwendung findet, gehen ihre zwingenden Bestimmungen vor, soweit erforderlich.

12.2 Sämtliche aus oder im Zusammenhang mit diesem ADV entstehenden Streitigkeiten unterliegen der ausschliesslichen Zuständigkeit der Gerichte des Kantons Zürich, Schweiz (erste Instanz: Bezirksgericht Zürich), sofern zwingendes Recht nichts anderes vorsieht. Diese Bestimmung lässt das Recht von Aufsichtsbehörden zur Untersuchung von Beschwerden und Durchsetzung des Datenschutzrechts unberührt.

Anhang 1 — Verarbeitete Personenbezogene Daten

Die folgende Tabelle führt die durch den Anbieter im Auftrag des Kunden im Zusammenhang mit dem Seamless-Produkt verarbeiteten Personenbezogenen Daten auf.

Kategorie	Details
Kategorien Personenbezogener Daten	Firmenname; Namen der Kontaktpersonen; Geschäftsadresse; Telefonnummer; E-Mail-Adresse; Vertragsdaten (Vertragsverhältnis, Produkt, Vertragsinteressen); Kundenhistorie, Vertragsabwicklung und Zahlungsdaten; Microsoft Entra ID Tenant ID; Microsoft Entra ID User Object IDs (für Telemetrie und Lizenzmanagement); primärer Kontaktname und E-Mail-Adresse des Seamless Admin; Anzeigename des Global Admin und Zustimmungsdatum; Audit-Logs (Authentifizierung gegenüber Seamless-Diensten); Daten zur Implementierung und Nutzung des Produkts; Aktivitätslogs zu Fehlersuche-Zwecken (maximal 90 Tage zu Sicherheits- und Diagnosezwecken aufbewahrt); Seamless-Konfigurationsdaten (Governance-Richtlinien, Vorlagen, Namenskonventionen, Genehmigungs-Workflows).
Kategorien betroffener Personen	Mitarbeitende (intern); Kontaktpersonen; Mitarbeitende externer Unternehmen; Interessenten; Administratoren und Benutzer der Microsoft-365-Umgebung des Kunden, die Seamless nutzen oder darüber verwaltet werden.

Kategorie	Details
Verarbeitungszwecke	Bereitstellung, Betrieb und Wartung des Seamless-Produkts und ergänzender Dienstleistungen unter den AGB (einschliesslich Erhebung, Verarbeitung, Analyse, Übertragung und Speicherung); Lizenzmanagement und Nutzungsverfolgung; Support und Fehlersuche; Sicherheitsüberwachung; KI-gestützte Verarbeitung Personenbezogener Daten (insbesondere E-Mail-Adressen) über Microsoft Azure AI Foundry zur Bereitstellung KI-gestützter Funktionen des Produkts; Erfüllung vertraglicher Verpflichtungen unter den AGB; soweit anwendbar, die Bereitstellung Exportierbarer Daten und Unterstützung von Switching und Interoperabilität gemäss dem Data Act.
Rechtsgrundlage	Die Verarbeitung ist zur Erfüllung der AGB erforderlich (Art. 6 Abs. 1 lit. b DSGVO; Art. 31 Abs. 2 lit. a revDSG).
Aufbewahrungsfrist	Audit-Logs (Authentifizierung): 30 Tage. Aktivitätslogs zur Fehlersuche: 90 Tage. Entra ID User Object IDs für Telemetrie: 90 Tage. Tenant ID und Admin-Kontaktdaten: für die Dauer der AGB zuzüglich gesetzlich vorgeschriebener Aufbewahrungsfristen. Seamless-Konfigurationsdaten: bis zur Löschung durch den Kunden über das Seamless Admin Center oder bis zur Beendigung der AGB.
Verarbeitungsorte	Personenbezogene Daten werden primär in der Schweiz gespeichert (Microsoft Azure Switzerland North). KI-gestützte Funktionen verarbeiten Personenbezogene Daten (insbesondere E-Mail-Adressen) über Microsoft Azure AI Foundry in Schweden, innerhalb des Europäischen Wirtschaftsraums. Statische, nicht-personenbezogene Inhalte werden global über Microsoft Azure CDN ausgeliefert. Sämtliche Verarbeitung Personenbezogener Daten erfolgt innerhalb des EWR oder der Schweiz.

Anhang 2 — Technische und organisatorische Massnahmen

Im Folgenden werden die wesentlichen technischen und organisatorischen Massnahmen zusammengefasst, die der Anbieter zur Sicherheit der unter diesem ADV verarbeiteten Personenbezogenen Daten umgesetzt hat.

A2.1 Zutrittskontrolle

Massnahmen zur Verhinderung des Zutritts unbefugter Personen zu Datenverarbeitungssystemen, mit denen Personenbezogene Daten verarbeitet werden.

Das Produkt ist ein PaaS-Dienst, der auf Microsoft Azure gehostet und durch Microsoft 365 ver-

waltet wird. Es besteht kein physischer Zugang zu solchen Umgebungen.

A2.2 Zugangskontrolle

Massnahmen zur Verhinderung der Nutzung von Datenverarbeitungssystemen durch unbefugte Personen:

- Zuweisung von Benutzerrechten und rollenbasierte Zugriffskontrollen
- Authentifizierung mit Benutzername/Passwort und zweitem Faktor (Multi-Faktor-Authentifizierung)
- Zugriffskontrolle über Conditional Access und Privileged Identity Management (PIM)
- Einsatz von Intrusion-Prevention-Systemen
- Weitere Massnahmen: Web-Application-Firewalls, regelmässige Schwachstellen-Scans, regelmässige Penetrationstests, Patch-Management, Mindestanforderungen an Passwort-Komplexität
- Verschlüsselung der Storage Accounts (AES-256)
- Hardware-Verschlüsselung für Notebooks
- Einsatz einer Software-Firewall (Office-Clients)

A2.3 Zugriffskontrolle

Massnahmen, damit die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und Personenbezogene Daten nicht unbefugt verarbeitet, genutzt oder gespeichert werden können:

- Erstellung eines Berechtigungskonzepts
- Reduzierung der Anzahl Administratoren auf das absolute Minimum
- Protokollierung von Anwendungszugriffen, insbesondere für Eingabe, Änderung und Datenlöschung
- Rechteverwaltung durch Systemadministratoren
- Passwortrichtlinie mit Vorgaben zu Passwortlänge und Passwortwechsel
- Entra ID User Object IDs werden als pseudonyme Kennungen anstelle von Namen oder E-Mail-Adressen verwendet

A2.4 Weitergabekontrolle

Massnahmen, damit Personenbezogene Daten bei der elektronischen Übertragung oder dem Transport bzw. der Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Dokumentation der Datenempfänger und Übertragungszeiten einschliesslich vereinbarter Löschzeiten
- Datenoffenlegung (nur) in anonymisierter oder verschlüsselter Form
- TLS-Verschlüsselung (1.2 oder höher) für sämtliche Kommunikation (Web-Client, APIs)

A2.5 Eingabekontrolle

Massnahmen, damit nachträglich überprüft werden kann, ob und durch wen Personenbezogene Daten in Datenverarbeitungssystemen eingegeben, geändert oder entfernt wurden:

- Protokollierung von Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Dateneingabe, -änderung und -löschung durch einzelne Benutzer
- Zuweisung von Rechten zur Eingabe, Änderung und Löschung von Daten basierend auf einem Berechtigungskonzept

A2.6 Auftragskontrolle

Massnahmen, damit Daten, die im Auftrag und in Übereinstimmung mit dem Verantwortlichen verarbeitet werden, nur entsprechend dessen Weisungen verarbeitet werden:

- Auswahl von Unterauftragsverarbeitern unter Berücksichtigung ihrer Historie (insbesondere zu Informationssicherheit)
- Schriftliche Weisungen an Unterauftragsverarbeiter
- Effektive Kontrollrechte, die durch Unterauftragsverarbeiter zugesichert werden
- Vorgängige Prüfung der Dokumentation und Sicherheitsmassnahmen der Unterauftragsverarbeiter
- Verpflichtung der Mitarbeitenden des Unterauftragsverarbeiters zur Vertraulichkeit
- Sichere Datenlöschung am Ende der Vertragsbeziehung
- Laufende Überwachung der Unterauftragsverarbeiter und ihrer Tätigkeiten

A2.7 Verfügbarkeitskontrolle

Massnahmen zum Schutz Personenbezogener Daten vor zufälliger Vernichtung oder Verlust:

- Das Produkt wird auf Microsoft Azure mit eingebauter Redundanz und Disaster Recovery gehostet
- Tests der Datenwiederherstellung
- Erstellung von Backup- und Recovery-Konzepten
- Erstellung eines Notfallplans
- Mehrere Rechenzentren in aktiver Konfiguration
- Verfügbarkeitszusagen sind in den AGB festgelegt (Abschnitt 10.2)

A2.8 Trennungsgrundsatz

Massnahmen, damit zu unterschiedlichen Zwecken erhobene Personenbezogene Daten getrennt verarbeitet werden können:

- Erstellung eines Berechtigungskonzepts
- Der Anbieter verarbeitet ausschliesslich die zur Bereitstellung des Produkts strikt erforderlichen Personenbezogenen Daten (Datenminimierung). Endbenutzer-Inhalte (Dokumente, Dateien, Kommunikation) werden vom Anbieter nicht verarbeitet oder gespeichert; sie verbleiben im Microsoft-365-Tenant des Kunden.

Anhang 3 — Liste der Unterauftragsverarbeiter

Unterauftragsverarbeiter	**Microsoft Ireland Operations Limited**
Sitz	Blackthorn Road, Dublin 18, Irland
Datenstandort	Schweiz (Azure Switzerland North); Schweden (Azure AI Foundry); globales Azure CDN für statische, nicht personenbezogene Inhalte

Unterauftragsverarbeiter	**Microsoft Ireland Operations Limited**
Verarbeitungszweck	Cloud-Infrastruktur und Hosting (Microsoft Azure); Identity Management und Authentifizierung (Microsoft Entra ID); Microsoft 365 Plattform-Integration (Microsoft Teams, SharePoint Online, Graph API); KI-gestützte Verarbeitung Personenbezogener Daten (insbesondere E-Mail-Adressen) über Microsoft Azure AI Foundry in Schweden; Commercial Marketplace Transaktionsabwicklung, Subscription Management und Billing (Azure Marketplace / Microsoft Marketplace), einschliesslich Offenlegung von Kundenkontaktinformationen und Transaktionsdetails an den Anbieter als Publisher gemäss den Microsoft Commercial Marketplace Terms of Use.
Übermittlungsmechanismus	EU-Entity (DSGVO direkt anwendbar); Verarbeitungsorte Schweiz und Schweden, beide als adäquat anerkannt bzw. innerhalb des EWR

Unterauftragsverarbeiter	**HubSpot Ireland Limited**
Sitz	1 Sir John Rogerson's Quay, Dublin 2, Irland
Datenstandort	EU / USA
Verarbeitungszweck	Customer Relationship Management (CRM); Kundenkommunikation und Support-Tracking; Marketing-Automation.
Übermittlungsmechanismus	EU-Entity; EU SCCs und Swiss SCCs für Übermittlungen in die USA

Unterauftragsverarbeiter	**Resend Inc.**
Sitz	375 Beale St Ste 300, San Francisco, CA 94105, USA
Datenstandort	USA / EU
Verarbeitungszweck	Versand transaktionaler E-Mails (z.B. Onboarding-Benachrichtigungen, System-Alerts, Produktkommunikation an Kunden und Benutzer).
Übermittlungsmechanismus	EU SCCs; Swiss SCCs

Unterauftragsverarbeiter	**Harvest**
Sitz	99 Wall Street Suite 1310, New York, NY 10005, USA
Datenstandort	USA
Verarbeitungszweck	Zeiterfassung und Rechnungsstellung für Direktrechnung ausserhalb des Marketplace (anwendbar auf Scale-Pläne mit Direktrechnung).
Übermittlungsmechanismus	EU SCCs; Swiss SCCs

Unterauftragsverarbeiter	**Google Ireland Limited**
Sitz	Gordon House, Barrow Street, Dublin 4, Irland
Datenstandort	EU / USA
Verarbeitungszweck	Website-Analyse (Google Analytics) zur Auswertung der Nutzung unserer Websites. IP-Anonymisierung ist aktiviert. Daten werden in pseudonymer Form erhoben.
Übermittlungsmechanismus	EU-Entity; EU SCCs und Swiss SCCs für Übermittlungen in die USA