

Auftragsverarbeitungsvertrag

Version 2.1, gültig ab 5. Oktober 2026

OutLine Digital Agency (Einzelunternehmer), Via Dalmazia 36, 76125 Trani (BT), Italien — USt-IdNr. IT08978680729

Wie wir als Ihr Auftragsverarbeiter die personenbezogenen Daten Ihrer Mitarbeitenden, Bewerbenden und sonstigen Beschäftigten verarbeiten, die Sie in Omega People eingeben: was wir damit tun dürfen, was nicht, und wie Übermittlungen abgesichert sind.

Rechtsgrundlagen

Verordnung (EU) 2016/679 (DSGVO), Art. 28 und Kapitel V ·
Durchführungsbeschluss (EU) 2021/914 der Kommission
(Standardvertragsklauseln) · UK GDPR und International Data Transfer
Addendum zu den EU-Standardvertragsklauseln · Bundesgesetz über den
Datenschutz (DSG), Art. 9 und 16 · California Consumer Privacy Act
(CCPA) und weitere Datenschutzgesetze der US-Bundesstaaten, soweit
anwendbar · Kanada: PIPEDA; Québec: Loi sur la protection des
renseignements personnels dans le secteur privé, Sections 17 und 18.3;
Alberta und British Columbia: Personal Information Protection Acts ·
Australien: Privacy Act 1988, Australian Privacy Principles 8 und 11 sowie
Part IIIC (meldepflichtige Datenschutzverletzungen) · Neuseeland: Privacy
Act 2020, Section 11 und Information Privacy Principles 5 und 12

Präambel

Dieser Vertrag ergänzt die Nutzungsbedingungen (<https://people.omegasuiteapp.com/legal/terms>) und regelt die Verarbeitung personenbezogener Daten, die OutLine Digital Agency (**der Auftragsverarbeiter**) im Auftrag des Kunden (**des Verantwortlichen**) bei der Erbringung von Omega People vornimmt.

Er bildet den nach Art. 28 Abs. 3 DSGVO erforderlichen Vertrag sowie — soweit der Verantwortliche ihnen unterliegt — den Vertrag nach Art. 28 der UK GDPR, Art. 9 des Schweizer Bundesgesetzes über den Datenschutz, Section 18.3 des Gesetzes von Québec über den Schutz personenbezogener Informationen im Privatsektor und den Datenschutzgesetzen der US-Bundesstaaten, die einen schriftlichen Vertrag mit einem Service Provider oder Auftragsverarbeiter verlangen. Er kommt zustande, wenn der Verantwortliche ihn bei der Eröffnung seines ersten Arbeitsbereichs annimmt, und bleibt in Kraft, solange der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Auftragsverarbeiter

OutLine Digital Agency (Einzelunternehmer), Via Dalmazia 36, 76125
Trani (BT), Italien — USt-IdNr. IT08978680729

Verantwortlicher

Der Kunde, wie im Konto und in den in der Anwendung hinterlegten
Unternehmensangaben bezeichnet.

Kontakt für Datenschutz

amministrazione@outlinedigital.it

Begriffe wie „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“ und „Verletzung des Schutzes personenbezogener Daten“ haben die Bedeutung nach der DSGVO; soweit ein anderes Gesetz gilt, umfassen sie die entsprechenden Begriffe dieses Gesetzes (etwa „business“ und „service provider“ nach dem CCPA).

Wer was entscheidet

Der Verantwortliche ist der Arbeitgeber. Er entscheidet, welche Daten er über seine Mitarbeitenden, Bewerbenden und sonstigen Beschäftigten erhebt, zu welchen Zwecken, auf welcher Rechtsgrundlage und wie lange, und er ist es, der sie informiert (seine eigene Datenschutzerklärung für das Personal). Der Auftragsverarbeiter stellt das Werkzeug bereit und trifft keine dieser Entscheidungen. Das bedeutet: Der Auftragsverarbeiter kann keine Daten auf Verlangen einer betroffenen Person löschen, und der Verantwortliche kann die Entscheidung, Daten erhoben zu haben, die er nicht hätte erheben dürfen, nicht auf den Auftragsverarbeiter abwälzen.

1. Verarbeitung auf dokumentierte Weisung

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten **ausschliesslich auf dokumentierte Weisung des Verantwortlichen**. Weisungen sind: dieser Vertrag, die Nutzungsbedingungen, die Dokumentation des Dienstes und die Einstellungen, die der Verantwortliche in der Anwendung vornimmt (Benutzer, Rollen und Berechtigungen, die von ihm eingeschalteten Module, Regeln für Stempelung und Standort, öffentliche Seiten, Integrationen, Aufbewahrungsfristen).
2. Der Auftragsverarbeiter verarbeitet die Daten nicht für eigene Zwecke, gibt sie nicht an Dritte weiter und verwendet sie weder für kommerzielle Auswertungen noch zum Training von Systemen der künstlichen Intelligenz.
3. Verpflichtet ihn eine gesetzliche Pflicht zu einer weiteren Verarbeitung, teilt der Auftragsverarbeiter dies dem Verantwortlichen vorher mit, sofern das Gesetz dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
4. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn eine Weisung seiner Auffassung nach gegen Datenschutzrecht verstösst.

2. Vertraulichkeit der befugten Personen

Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung befugten Personen — Mitarbeitende und Auftragnehmer — einer über das Ende ihrer Tätigkeit hinaus fortbestehenden Vertraulichkeitspflicht unterliegen, Weisungen erhalten und nur auf die für ihre Aufgabe erforderlichen Daten zugreifen.

Support-Mitarbeitende greifen auf Arbeitsbereiche von Kunden nur über den in Abschnitt 8 beschriebenen **protokollierten befristeten Zugang** zu.

3. Sicherheitsmassnahmen

Der Auftragsverarbeiter setzt die in **Anhang B** und auf der Seite Sicherheitsmassnahmen (<https://people.omegasuiteapp.com/legal/security>) beschriebenen technischen und organisatorischen Massnahmen um, die Bestandteil dieses Vertrags sind.

Die Massnahmen können im Laufe der Zeit angepasst werden, sofern das Sicherheitsniveau nicht sinkt. Wesentliche Änderungen werden dem Verantwortlichen mit derselben Frist wie bei Unterauftragsverarbeitern mitgeteilt.

4. Unterauftragsverarbeiter

Der Verantwortliche erteilt dem Auftragsverarbeiter eine **allgemeine Genehmigung**, unter folgenden Bedingungen weitere Auftragsverarbeiter einzusetzen.

1. Die aktuelle Liste ist auf der Seite Unterauftragsverarbeiter (<https://people.omegasuiteapp.com/legal/subprocessors>) veröffentlicht.
2. Jeder Unterauftragsverarbeiter ist vertraglich an Datenschutzpflichten gebunden, die denen dieses Vertrags gleichwertig sind; der Auftragsverarbeiter haftet für dessen Leistung wie für die eigene.
3. Die Hinzunahme oder der Austausch eines Unterauftragsverarbeiters wird dem Verantwortlichen mindestens **30 Tage** im Voraus per E-Mail und gut sichtbar in der Anwendung mitgeteilt.
4. Innerhalb dieser Frist kann der Verantwortliche aus vernünftigen, belegten Datenschutzgründen widersprechen.

Bei Widerspruch suchen die Parteien in gutem Glauben nach einer Alternative; ist keine praktikabel, kann der Verantwortliche ohne Vertragsstrafe mit Wirkung zum Zeitpunkt der Änderung kündigen.

Unterauftragsverarbeiter	Tätigkeit	Land
IONOS SE	Server und Speicher: betreibt die Anwendung, die Datenbanken der Arbeitsbereiche, hochgeladene Dateien (Personaldokumente, Lohnabrechnungen, Belege, Anhänge) und Sicherungskopien.	Deutschland
Aruba S.p.A.	Leitet die ausgehenden E-Mails des Dienstes weiter: Einladungen an Mitarbeitende und Teammitglieder, Passwort-Zurücksetzungen, Nachrichten an Bewerbende, E-Mails aus den vom Kunden eingerichteten Automatisierungsregeln sowie E-Mails zum Abonnement. Die Nachrichten enthalten Name und E-Mail-Adresse des Empfängers sowie den Inhalt der Nachricht.	Italien
Stripe Payments Europe, Limited	Zieht die Abonnemententgelte ein und stellt Zahlungsbelege aus. Verarbeitet nur die Rechnungsdaten des Abonnenten (Firmenname, Anschrift, USt-IdNr., Rechnungs-E-Mail, Kartendaten – die nie über unsere Server laufen). Dazu erhält es den Namen des Arbeitsbereichs, die Anmelde-E-Mail-Adresse seines Inhabers und unsere internen Referenznummern. Kein Zugriff auf die Daten in den Arbeitsbereichen.	Irland

Massgeblich ist die laufend aktualisierte Fassung unter [/legal/subprocessors](https://people.omegasuiteapp.com/legal/subprocessors) (<https://people.omegasuiteapp.com/legal/subprocessors>): Diese Tabelle ist eine unverbindliche Kopie zum Zeitpunkt der Erstellung dieses Dokuments.

Von Ihnen verbundene Dienste sind nicht unsere Unterauftragsverarbeiter

Verbindet der Verantwortliche Omega People mit anderen Diensten — einem Anbieter für elektronische Signaturen (Yousign) mit eigenem Konto und API-Schlüssel, einem Anbieter künstlicher Intelligenz mit eigenem Schlüssel oder Webhooks, die seine Automatisierungsregeln aufrufen —, gelangen die an sie gesendeten Daten auf Weisung des Verantwortlichen und gemäss dessen Vertrag mit dem jeweiligen Anbieter dorthin. Diese Anbieter sind Auftragsverarbeiter des Verantwortlichen, nicht Unterauftragsverarbeiter des Auftragsverarbeiters. In der Anwendung findet der Verantwortliche unter **Einstellungen -> Datenschutz und Compliance** sein bereits ausgefülltes Verzeichnis der Verarbeitungstätigkeiten, die Liste der von ihm verbundenen Dienste sowie die Datenschutzhinweise für seine Mitarbeitenden und Bewerbenden.

5. Unterstützung bei Anfragen betroffener Personen

Die Anwendung gibt dem Verantwortlichen die Werkzeuge, die Anfragen seiner Mitarbeitenden, ehemaligen Mitarbeitenden und Bewerbenden selbst und ohne Wartezeit zu beantworten: Suche, Export aller über eine Mitarbeitende oder einen Mitarbeitenden geführten Daten, Berichtigung, Löschung und ein Protokoll der Änderungen an Personaldaten. Mitarbeitende mit Zugang zum persönlichen Bereich können ihre eigenen Anwesenheiten, Abwesenheiten, Schichten, Dokumente und Lohnabrechnungen direkt einsehen.

Wendet sich eine Mitarbeitende, ein Mitarbeitender, eine Bewerbende, ein Bewerbender oder eine andere betroffene Person direkt an den Auftragsverarbeiter, **bearbeitet dieser die Anfrage nicht**, sondern leitet sie unverzüglich an den Verantwortlichen weiter und teilt der Person mit, dass der Verantwortliche ihr Arbeitgeber (bzw. das Unternehmen, bei dem sie sich beworben hat) ist.

Reichen die Werkzeuge der Anwendung nicht aus, leistet der Auftragsverarbeiter angemessene technische Unterstützung, auf eigene Kosten, wenn der Bedarf auf eine Fehlfunktion zurückgeht.

6. Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes der in seinem Auftrag verarbeiteten personenbezogenen Daten **unverzüglich und in jedem Fall innerhalb von 48 Stunden**, nachdem sie ihm bekannt geworden ist, und strebt eine Meldung innerhalb von 24 Stunden an. Eine erste Meldung erfolgt auch dann, wenn noch nicht alle Informationen vorliegen; die übrigen folgen schrittweise, sobald sie bekannt sind.
2. Die Meldung beschreibt die Art der Verletzung, die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Massnahmen, damit der Verantwortliche beurteilen kann, ob und wann er die zuständigen Behörden und die betroffenen Personen innerhalb der Fristen des für ihn geltenden Rechts benachrichtigt (zum Beispiel 72 Stunden nach DSGVO und UK GDPR oder „so rasch als möglich“ bzw. „sobald praktikabel“ nach dem Schweizer DSG, PIPEDA und den australischen und neuseeländischen Regelungen).
3. Der Auftragsverarbeiter dokumentiert jede Verletzung und leistet dem Verantwortlichen die Mitwirkung, die dieser zur Erfüllung seiner Pflichten gegenüber Behörden und betroffenen Personen benötigt.
4. Die Benachrichtigung von Behörden und betroffenen Personen bleibt Aufgabe des Verantwortlichen: Der Auftragsverarbeiter nimmt sie nicht an dessen Stelle vor.

7. Datenschutz-Folgenabschätzung und vorherige Konsultation

Unter Berücksichtigung der Art der Verarbeitung und der ihm vorliegenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen bei Datenschutz-Folgenabschätzungen und einer etwaigen vorherigen Konsultation einer Behörde, indem er technische Unterlagen zur Architektur, zu den Sicherheitsmassnahmen und zu den Datenflüssen des Dienstes bereitstellt.

Wann sich eine Folgenabschätzung lohnt

HR-Software verarbeitet Daten über Menschen, deren Lebensunterhalt vom Verantwortlichen abhängt, und mehrere Funktionen von Omega People verdienen Aufmerksamkeit: die **Zeiterfassung mit Geolokalisierung**, die festhält, wo sich eine Mitarbeitende oder ein Mitarbeitender beim Ein- oder Ausstempeln befindet; **Gesundheitsdaten** in Arbeitsunfähigkeitsbescheinigungen, Aufzeichnungen über ärztliche Untersuchungen und Unfallmeldungen; **Mitarbeiterbeurteilungen und Disziplinarunterlagen**; die **Meldestelle**; sowie jede Nutzung von **KI-Funktionen** auf Daten von Mitarbeitenden. In vielen Ländern ist dies zudem arbeitsrechtlich bzw. durch Vorschriften zur Überwachung am Arbeitsplatz geregelt (vorherige Information der Mitarbeitenden, Konsultation der Arbeitnehmervertretung oder eines Betriebsrats). Die Anwendung weist unter **Einstellungen** -> **Datenschutz und Compliance** darauf hin, die Abschätzung führt jedoch der Verantwortliche durch.

8. Support-Zugriff auf den Arbeitsbereich

- Er erfolgt nur auf Verlangen des Verantwortlichen oder für technische Arbeiten, die erforderlich sind, um den Dienst in Betrieb zu halten oder eine Störung zu beheben.
- Er nutzt einen im Arbeitsbereich angelegten **eigenen, befristeten Zugang**, der nach **15 Minuten** automatisch abläuft: Er verwendet die Zugangsdaten der Benutzer des Verantwortlichen weder noch kennt er sie.
- Solange er besteht, hat dieser Zugang die Rechte eines Administrators des Arbeitsbereichs: Nur so lässt sich ein Problem so sehen, wie der Verantwortliche es sieht. Die Person, die ihn nutzt, ist zur Vertraulichkeit verpflichtet (Abschnitt 2) und sieht nur ein, was die Anfrage erfordert.
- Er wird **protokolliert und ist für den Verantwortlichen einsehbar**. Jeder Zugriff wird mit Person, Zeitpunkt,

Dauer und Grund festgehalten; der Kontoinhaber des Verantwortlichen erhält bei Beginn sofort eine E-Mail, und Inhaber und Administratoren des Verantwortlichen können das Protokoll jederzeit unter Einstellungen -> Supportzugriffe einsehen. Während des Zugriffs sind Exporte, Datei-Downloads sowie Änderungen an Passwörtern, Anmeldeadressen und API-Schlüsseln gesperrt; jeder Versuch erscheint im Protokoll.

9. Prüfungen und Nachweis der Einhaltung

Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags erforderlich sind, und ermöglicht Prüfungen einschliesslich Inspektionen durch den Verantwortlichen oder einen von ihm beauftragten Prüfer.

1. Prüfungen sind mindestens 15 Tage im Voraus anzukündigen, finden während der Geschäftszeiten statt und dürfen weder die Kontinuität des Dienstes noch die Vertraulichkeit der Daten anderer Kunden beeinträchtigen.
2. Zulässig ist **eine Prüfung pro Kalenderjahr**, zuzüglich weiterer Prüfungen nach einer Verletzung des Schutzes personenbezogener Daten oder auf begründetes Verlangen einer Aufsichtsbehörde.
3. Der Prüfer des Verantwortlichen darf kein Wettbewerber des Auftragsverarbeiters sein und muss eine Vertraulichkeitsverpflichtung unterzeichnen.
4. Die Kosten zusätzlicher, vom Verantwortlichen verlangter Prüfungen trägt der Verantwortliche, es sei denn, die Prüfung deckt einen Verstoß des Auftragsverarbeiters auf.

Der Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungen, die er im Auftrag des Verantwortlichen durchführt (Art. 30 Abs. 2 DSGVO), und arbeitet auf Anfrage mit den Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben zusammen.

10. Internationale Übermittlungen

Der Auftragsverarbeiter verarbeitet die Daten innerhalb des Europäischen Wirtschaftsraums: Die Infrastruktur wird von IONOS SE in Deutschland betrieben, und seine Unterauftragsverarbeiter sitzen in der Europäischen Union. **Er übermittelt die Daten nicht in Drittländer**, ausser um sie dem Verantwortlichen und dessen Benutzern dort zugänglich zu machen, wo sie sich befinden.

1. **Aus der EU an den Verantwortlichen.** Soweit die DSGVO auf die Bereitstellung von Daten an einen Verantwortlichen Anwendung findet, der für diese Daten nicht von einem Angemessenheitsbeschluss der EU erfasst ist, vereinbaren die Parteien die EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/914 der Kommission), **Modul vier** (Auftragsverarbeiter an Verantwortlichen), die durch Verweis Bestandteil dieses Vertrags sind. Anwendbares Recht und Gerichtsstand richten sich nach Artikel 23 der Nutzungsbedingungen; die Einzelheiten der Verarbeitung ergeben sich aus Anhang A. Für diese Klauseln gilt: Die Kopplungsklausel (Klausel 7) findet keine Anwendung; die Klauseln 14 und 15 gelten nur, wenn der Auftragsverarbeiter die vom Verantwortlichen erhaltenen Daten mit personenbezogenen Daten verbindet, die er in der Europäischen Union erhoben hat, was nicht der Fall ist; es gilt italienisches Recht (Klausel 17), und zuständig sind die Gerichte Italiens (Klausel 18); Parteien sind die in der Präambel genannten, und Anhang I entspricht Anhang A dieses Vertrags. Die Bereitstellung von Daten an einen Verantwortlichen im Vereinigten Königreich, in der Schweiz oder in Neuseeland stützt sich auf die Angemessenheitsbeschlüsse der Europäischen Kommission für diese Länder, solange sie in Kraft sind; dasselbe gilt für einen Verantwortlichen in Kanada, soweit PIPEDA auf die betreffenden Daten anwendbar ist, und für einen Verantwortlichen in den Vereinigten Staaten, soweit er für diese Daten nach dem EU-U.S. Data Privacy Framework zertifiziert ist. In allen anderen Fällen gilt Modul vier.
2. **Vereinigtes Königreich.** Für einen Verantwortlichen, der der UK GDPR unterliegt, stützen sich Übermittlungen an den Auftragsverarbeiter auf die Angemessenheitsregelungen des Vereinigten Königreichs für den Europäischen Wirtschaftsraum. Sollten diese entfallen, vereinbaren die Parteien die EU-Standardvertragsklauseln (Modul zwei) zusammen mit dem vom Information Commissioner herausgegebenen britischen **International Data Transfer Addendum**, die durch Verweis einbezogen werden.
3. **Schweiz.** Für einen Verantwortlichen, der dem Schweizer DSG unterliegt, stützen sich Übermittlungen an den Auftragsverarbeiter auf die Anerkennung der Angemessenheit der betreffenden Staaten durch den Bundesrat. Sollte diese entfallen, vereinbaren die Parteien die EU-Standardvertragsklauseln mit den für die Schweiz erforderlichen Anpassungen: Der EDÖB ist die zuständige Aufsichtsbehörde für Übermittlungen nach Schweizer Recht, und „Mitgliedstaat“ umfasst für die Rechte der betroffenen Personen auch die Schweiz.

4. Sollte für einen Unterauftragsverarbeiter jemals eine Übermittlung ausserhalb des EWR erforderlich werden, kündigt der Auftragsverarbeiter dies gemäss Abschnitt 4 an und nimmt sie nur mit einer der Garantien nach Kapitel V der DSGVO vor, die er in der Liste der Unterauftragsverarbeiter angibt.
5. Übermittlungen, die sich aus vom Verantwortlichen verbundenen Diensten ergeben (zum Beispiel einem ausserhalb des EWR niedergelassenen KI-Anbieter oder Anbieter für elektronische Signaturen), erfolgen in dessen Verantwortung.
6. **Behördliche Anfragen.** Verlangt ein Gericht oder eine Behörde vom Auftragsverarbeiter Zugang zu den Daten des Verantwortlichen, prüft der Auftragsverarbeiter die Rechtmässigkeit des Ersuchens, ficht es an, wenn dafür vernünftige Gründe bestehen, gibt nur heraus, was unbedingt erforderlich ist, und unterrichtet den Verantwortlichen vorab, sofern das Gesetz dies nicht verbietet.

11. Vereinigte Staaten: Bestimmungen für Service Provider

Ist der Verantwortliche ein „business“ im Sinne des California Consumer Privacy Act (CCPA) oder ein „controller“ im Sinne eines anderen Datenschutzgesetzes eines US-Bundesstaats, handelt der Auftragsverarbeiter als dessen **Service Provider** (bzw. Processor). Der Verantwortliche legt dem Auftragsverarbeiter die personenbezogenen Informationen nur für den begrenzten und festgelegten Geschäftszweck offen, den in Anhang A beschriebenen Dienst zu erbringen, und der Auftragsverarbeiter:

- verkauft oder teilt die personenbezogenen Informationen nicht und verwendet sie nicht für kontextübergreifende verhaltensbasierte oder zielgerichtete Werbung;
- speichert, verwendet oder offenbart sie zu keinem anderen — auch keinem anderen kommerziellen — Zweck als der vertragsgemässen Erbringung des Dienstes und nicht ausserhalb der unmittelbaren Geschäftsbeziehung mit dem Verantwortlichen;
- führt sie nicht mit personenbezogenen Informationen zusammen, die er aus einer anderen Quelle erhält oder aus eigenen Kontakten mit der betroffenen Person erhebt, soweit diese Gesetze dies einem Service Provider nicht erlauben;
- erfüllt die Pflichten, die diese Gesetze Service Providern und Auftragsverarbeitern auferlegen, und gewährleistet für die personenbezogenen Informationen das von ihnen verlangte Datenschutzniveau, einschliesslich der Sicherheitsmassnahmen in Anhang B;
- benachrichtigt den Verantwortlichen **innerhalb von fünf Geschäftstagen**, wenn er feststellt, dass er diese Pflichten nicht mehr erfüllen kann;
- ermöglicht dem Verantwortlichen, angemessene und geeignete Schritte zu unternehmen, um sicherzustellen, dass die Informationen im Einklang mit den eigenen Pflichten des Verantwortlichen verwendet werden (Abschnitte 3 und 9), und nach Mitteilung eine unbefugte Verwendung zu beenden und zu beheben;
- unterstützt den Verantwortlichen bei der Beantwortung von Anfragen betroffener Personen (Abschnitt 5) und verpflichtet seine Unterauftragsverarbeiter durch schriftlichen Vertrag auf dieselben Pflichten (Abschnitt 4);
- behandelt die Informationen vertraulich und löscht sie am Ende des Dienstes oder gibt sie zurück (Abschnitt 13).

Keine geschützten Gesundheitsinformationen, keine biometrischen Merkmale. Der Auftragsverarbeiter ist kein „business associate“ im Sinne des HIPAA und hat keine entsprechende Vereinbarung (business associate agreement) unterzeichnet: Der Dienst darf nicht verwendet werden, um geschützte Gesundheitsinformationen (protected health information) eines Krankenversicherungsplans oder eines Gesundheitsdienstleisters zu führen. Unterlagen, die ein Arbeitgeber in seiner Eigenschaft als Arbeitgeber führt — eine Arbeitsunfähigkeitsbescheinigung, eine Bescheinigung der Arbeitsfähigkeit —, sind keine geschützten Gesundheitsinformationen; die Vertraulichkeitsregeln für medizinische Unterlagen von Beschäftigten (zum Beispiel nach ADA, FMLA und GINA) hat der Verantwortliche mit den Zugriffsrechten des Dienstes umzusetzen. Der Dienst erfasst keine Fingerabdrücke, keine Scans der Gesichts- oder Handgeometrie, keine Stimmabdrücke und keine anderen biometrischen Merkmale — die Kamera dient nur dazu, einen QR-Code zu lesen und Dokumente zu fotografieren —, und der Verantwortliche darf keine solchen Daten hochladen.

Sicherheitsvorfälle. Abschnitt 6 deckt auch die Benachrichtigung ab, die die Gesetze der US-Bundesstaaten von einem Unternehmen verlangen, das Daten im Auftrag ihres Inhabers führt.

12. Kanada, Australien und Neuseeland

Für einen Verantwortlichen, der einem der folgenden Gesetze unterliegt, verarbeitet der Auftragsverarbeiter die Daten nur zur Erbringung des Dienstes, schützt sie mit den in diesem Vertrag beschriebenen Garantien und unterstützt den Verantwortlichen wie in den Abschnitten 5 bis 9 beschrieben. Zusätzlich gilt:

Kanada (PIPEDA sowie die Personal Information Protection Acts von Alberta und British Columbia)

Der Verantwortliche bleibt für die personenbezogenen Informationen verantwortlich, die er dem Auftragsverarbeiter zur Verarbeitung anvertraut. Der Auftragsverarbeiter verwendet sie nur für die Zwecke des Dienstes, gewährt ihnen einen Schutz, der dem vom Verantwortlichen geschuldeten vergleichbar ist, und unterrichtet den Verantwortlichen nach Abschnitt 6 über jede Verletzung der Sicherheitsvorkehrungen, damit dieser beurteilen kann, ob ein tatsächliches Risiko eines erheblichen Schadens besteht, die Verletzung melden und sein Verzeichnis der Verletzungen führen kann. **Die Informationen werden ausserhalb Kanadas gespeichert und verarbeitet** — in den Ländern, die in der Liste der Unterauftragsverarbeiter (<https://people.omegasuiteapp.com/legal/subprocessors>) angegeben sind —, wo sie dem Recht dieser Länder unterliegen und deren Gerichten und Behörden nach diesem Recht zugänglich sein können; die betroffenen Personen darüber zu informieren und diese Länder zu nennen, wo das Gesetz es verlangt (etwa in Alberta), ist Aufgabe des Verantwortlichen.

Québec

Dieser Vertrag ist der schriftliche Vertrag nach Section 18.3 des Gesetzes über den Schutz personenbezogener Informationen im Privatsektor (Loi sur la protection des renseignements personnels dans le secteur privé). Der Auftragsverarbeiter verwendet die personenbezogenen Informationen nur zur Erbringung des Dienstes; wendet zum Schutz ihrer Vertraulichkeit die Massnahmen in Anhang B an; bewahrt sie nach Vertragsende nicht auf (Abschnitt 13); unterrichtet die beim Verantwortlichen für den Schutz personenbezogener Informationen zuständige Person **unverzüglich über jede Verletzung oder versuchte Verletzung** einer Pflicht zur Vertraulichkeit dieser Informationen, gleich durch wen; und ermöglicht dieser Person jede Überprüfung in Bezug auf die Vertraulichkeit (Abschnitt 9). Bevor Informationen ausserhalb Québecks weitergegeben werden, muss der Verantwortliche die nach Section 17 dieses Gesetzes vorgeschriebene Datenschutz-Folgenabschätzung durchführen: Der Auftragsverarbeiter stellt ihm die dafür nötigen Angaben bereit — wo die Daten gespeichert sind, wer die Unterauftragsverarbeiter sind, welche Sicherheitsmassnahmen gelten und welcher Rechtsrahmen in der Europäischen Union anwendbar ist.

Der Verantwortliche behält die tatsächliche Kontrolle über die personenbezogenen Informationen: Er bestimmt, wer darauf zugreifen darf, und kann jederzeit darauf zugreifen, sie ändern, abrufen und löschen; der Auftragsverarbeiter verarbeitet sie nur, um sie zu speichern und dem Verantwortlichen und dessen Benutzern zugänglich zu machen, und verpflichtet seine Unterauftragsverarbeiter auf dieselben Pflichten. Auf dieser Grundlage soll die Bereitstellung der Informationen an den Auftragsverarbeiter eine *Nutzung* (use) durch den Verantwortlichen und keine *Offenlegung* (disclosure) im Sinne des Australian Privacy Principle 8 sein; ob sie das ist, hat der Verantwortliche zu beurteilen. Hat der Auftragsverarbeiter hinreichende Gründe für den Verdacht eines unbefugten Zugriffs auf die Informationen, ihrer unbefugten Offenlegung oder ihres Verlusts, benachrichtigt er den Verantwortlichen nach Abschnitt 6, damit dieser seine Bewertung innerhalb der 30 Tage abschliessen kann, die die Regelung zu meldepflichtigen Datenschutzverletzungen (Notifiable Data Breaches scheme) vorsieht; die Parteien vereinbaren, dass eine Meldung an das Office of the Australian Information Commissioner und an die betroffenen Personen durch den Verantwortlichen erfolgt.

Der Auftragsverarbeiter hält die personenbezogenen Informationen als Beauftragter (agent) des Verantwortlichen zur sicheren Verwahrung und Verarbeitung und verwendet oder offenbart sie nicht für eigene Zwecke: Nach Section 11 des Privacy Act 2020 gelten die Informationen als vom Verantwortlichen gehalten, der für sie verantwortlich bleibt, und ihre Übermittlung an den Auftragsverarbeiter ist keine Offenlegung ausserhalb Neuseelands im Sinne des Information Privacy Principle 12. Der Auftragsverarbeiter meldet Datenschutzverletzungen nach Abschnitt 6, damit der Verantwortliche den Privacy Commissioner und die betroffenen Personen so bald wie praktikabel benachrichtigen kann, wenn ein ernsthafter Schaden wahrscheinlich ist.

13. Was am Ende geschieht

1. Der Verantwortliche kann die Daten während der gesamten Vertragsbeziehung selbst in offenen Formaten exportieren.
2. Nach Vertragsende bleibt der Arbeitsbereich **30 Tage** lang im Nur-Lese-Modus zugänglich, um den Export zu ermöglichen.
3. Nach Ablauf dieser Frist **löscht** der Auftragsverarbeiter die personenbezogenen Daten unverzüglich, spätestens jedoch innerhalb der folgenden 30 Tage; Kopien in Sicherungen bestehen nicht mehr, sobald die Rotation abgelaufen ist, spätestens etwa drei Monate nach der Löschung. Länger werden Daten nur aufbewahrt, soweit das Recht der Union oder eines Mitgliedstaats dies verlangt.
4. Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung schriftlich.
5. Die gesetzliche Aufbewahrung von Unterlagen zu Arbeitsverhältnis, Lohn, Arbeitszeit sowie Arbeitssicherheit und Gesundheitsschutz ist eine Pflicht des Verantwortlichen als Arbeitgeber: Der Verantwortliche exportiert, was er aufbewahren muss, bevor der Exportzeitraum endet. Der Auftragsverarbeiter dient dem Verantwortlichen nach Vertragsende nicht als Archiv.

14. Rangfolge

Bei Widersprüchen gehen die Standardvertragsklauseln (soweit anwendbar) diesem Vertrag vor, und dieser Vertrag geht in Bezug auf personenbezogene Daten den Nutzungsbedingungen vor. Die Haftung richtet sich nach den Nutzungsbedingungen.

Anhang A — Einzelheiten der Verarbeitung

Gegenstand	Bereitstellung eines Online-Dienstes für das Personalmanagement: Personalakten, Zeiterfassung und Anwesenheit, Schichten, Ferien und Abwesenheiten, Dokumente und elektronische Signatur, Spesen, Lohnvorbereitung, Recruiting, Weiterbildung, Arbeitssicherheit und Gesundheitsschutz, Mitarbeiterbeurteilungen, Meldestelle, interne Kommunikation.
Dauer	Die Laufzeit des Dienstleistungsvertrags zuzüglich des 30-tägigen Exportzeitraums.
Aufbewahrung während der Laufzeit	Die Daten werden so lange aufbewahrt, wie der Verantwortliche sie im Arbeitsbereich belässt. Der Verantwortliche legt die Aufbewahrungsfristen fest und löscht Einträge selbst (zum Beispiel ehemalige Mitarbeitende, nicht berücksichtigte Bewerbende, abgeschlossene Meldungen der Meldestelle, für die sich eine automatische Bereinigung nach einer vom Verantwortlichen gewählten Frist einschalten lässt). Während der Laufzeit löscht der Auftragsverarbeiter Daten des Arbeitsbereichs nur in den Fällen aus eigener Initiative, die die Anwendung vorsieht und die der Verantwortliche anpassen kann: Bewerbungen nicht berücksichtigter Bewerbender werden nach der in den Recruiting-Einstellungen festgelegten Frist gelöscht (standardmässig 12 Monate), und Registrierungen mobiler Geräte, die 180 Tage lang nicht genutzt wurden, werden entfernt.
Art und Zweck	Erheben, Erfassen, Organisieren, Ordnen, Speichern, Auslesen, Abfragen, Übermitteln an die vom Verantwortlichen eingerichteten Dienste, Löschen — ausschliesslich, um die Anwendung so zu betreiben, wie der Verantwortliche sie eingerichtet hat.
Häufigkeit	Fortlaufend, solange der Dienst genutzt wird.

Kategorien betroffener Personen — je nachdem, wie der Verantwortliche den Dienst nutzt:

- Mitarbeitende, Arbeitnehmende, Lernende, Praktikantinnen und Praktikanten sowie sonstige Beschäftigte des Verantwortlichen, einschliesslich **ehemaliger Beschäftigter**, deren Akten der Verantwortliche aufbewahrt;
- **Bewerbende**, die sich über die Karriereseite des Verantwortlichen bewerben oder die der Verantwortliche erfasst;
- Auftragnehmer, Leiharbeitnehmende und andere Personen, die der Verantwortliche im Arbeitsbereich verwaltet;
- Inhaber/innen, Administratorinnen und Administratoren sowie Vorgesetzte des Verantwortlichen, die den Dienst nutzen;
- von Mitarbeitenden angegebene **Notfallkontakte** sowie Familienangehörige, soweit der Verantwortliche sie erfasst (zum Beispiel in Nachweisen für familienbedingte Abwesenheiten);
- Personen, die über die Meldestelle eine Meldung senden (und anonym bleiben können), sowie in einer Meldung genannte Personen;
- andere Personen, die in Dokumenten, Nachrichten, Spesenabrechnungen, Unfallmeldungen und Notizen genannt werden.

Kategorien personenbezogener Daten:

Kategorie	Beispiele	Wo sie vorkommt
Identifikations- und Kontaktdaten	Name, Geburtsdatum und -ort, Geschlecht, Wohnadresse, E-Mail-Adresse, Telefonnummer, Notfallkontakt	Personalakten, persönlicher Bereich

Amtliche Kennungen	Sozialversicherungs- oder Steuernummern, Nummer und Ablaufdatum des Ausweisdokuments	Personalakten, Onboarding
Beschäftigungsdaten	Funktion, Abteilung, Standort, Vorgesetzte/r, Vertragsart und -daten, Probezeit, Kündigungsfrist, Austrittsdatum und -grund, Kompetenzen, überlassene Ausrüstung	Personalakten, Verträge, Organigramm, Ausrüstung
Vergütungs- und Finanzdaten	Gehalt und Lohnbestandteile, Bankverbindung, Spesen und Erstattungen, Zusatzleistungen, vom Verantwortlichen hochgeladene Lohnabrechnungen	Lohnvorbereitung, Spesen, Zusatzleistungen, Dokumente
Arbeitszeitdaten	Ein- und Ausstempelzeiten, Zeitrachweise, Schichten, Verfügbarkeiten, Überstunden, Bereitschaft, Stunden nach Projekt	Anwesenheit, Schichtplanung, Projekte
Standortdaten	die Position des Geräts im Moment des Ein- oder Ausstempelns (Koordinaten, Genauigkeit, ob sie innerhalb des für den Standort festgelegten Bereichs liegt), nur wenn der Verantwortliche den Standort für Stempelungen einschaltet. Es findet keine fortlaufende Ortung statt.	Anwesenheit
Ferien- und Abwesenheitsdaten	Art, Daten und Grund der Abwesenheiten, Saldi, Nachweise	Ferien und Abwesenheiten
Leistungs- und Entwicklungsdaten	Beurteilungen, Selbsteinschätzungen, Ziele, besuchte Weiterbildungen und Zertifikate, Umfrageantworten (anonym, wo der Verantwortliche dies so einstellt)	Beurteilungen, Weiterbildung, Umfragen
Disziplinardaten	Vorwürfe, die Stellungnahme der oder des Mitarbeitenden, Ergebnis	Personalakten
Bewerberdaten	Name, Kontaktdaten, Lebenslauf und Begleitnachricht, Phase des Auswahlverfahrens, Notizen und Bewertung	Recruiting, Karriereseite
Meldungen der Meldestelle	Inhalt der Meldung und der Folgenachrichten, Anhänge, Namen der betroffenen Personen. Die meldende Person wird vom System nicht identifiziert: Der Zugang zur Weiterverfolgung erfolgt über einen einmal angezeigten Code, von dem nur ein Fingerabdruck gespeichert wird.	Meldestelle
Dokumente und Freitext	Verträge, unterzeichnete Dokumente, Bescheinigungen, Schreiben, Nachrichten im Team-Chat, Mitteilungen und Kommentare, Dateien in der gemeinsamen Ablage	Dokumente, Chat, Mitteilungen, Ablage
Nutzungs- und Sicherheitsdaten	Anmeldungen, Sitzungen, für die mobile App oder das Terminal registrierte Geräte, Protokoll der Änderungen an Personaldaten	Aktivitäts- und Änderungsprotokolle

Besondere Kategorien (Art. 9 DSGVO)
und ähnlich sensible Daten

Gesundheitsdaten
(Arbeitsunfähigkeitsbescheinigungen und
Abwesenheitsgründe,
arbeitsmedizinische Untersuchungen mit
Ergebnis und Auflagen, Arbeitsunfälle
und Verletzungen); Daten, aus denen die
Gewerkschaftszugehörigkeit
hervorgehen kann (Abwesenheiten für
Gewerkschaftstätigkeit oder Streiks); alle
anderen sensiblen Daten — etwa zu
Religion, ethnischer Herkunft,
Behinderung oder Vorstrafen —, die der
Verantwortliche erfassen will oder die in
den von ihm hochgeladenen
Dokumenten enthalten sind

Ferien und Abwesenheiten,
Arbeitssicherheit, Dokumente,
Lohnvorbereitung

Besondere Kategorien: Der Verantwortliche entscheidet und steht dafür ein

Ein HR-System enthält seiner Natur nach besondere Kategorien von Daten. Ob sie erfasst werden, auf welcher Rechtsgrundlage (zum Beispiel den Pflichten des Arbeitgebers nach Arbeits-, Sozialversicherungs- und Arbeitsschutzrecht), wer sie sehen darf und wie lange, entscheidet der Verantwortliche; er ist dafür verantwortlich, sie auf das notwendige Minimum zu beschränken: erfassen, dass eine Mitarbeitende oder ein Mitarbeitender arbeitsunfähig oder abwesend ist, nicht die Diagnose, wo immer das Gesetz nicht mehr verlangt. Der Auftragsverarbeiter verlangt, liest oder nutzt diese Daten zu keinem anderen Zweck, als sie zu speichern und den vom Verantwortlichen berechtigten Benutzern anzuzeigen.

Anhang B — Sicherheitsmassnahmen

Die technischen und organisatorischen Massnahmen des Auftragsverarbeiters sind ausführlich auf der Seite Sicherheitsmassnahmen (<https://people.omegasuiteapp.com/legal/security>) beschrieben, die Bestandteil dieses Vertrags ist. Kurz: eine eigene Datenbank pro Arbeitsbereich, verschlüsselte Übertragung, verschlüsselte Speicherung der Zugangsdaten verbundener Dienste und des API-Schlüssels eines KI-Anbieters, Passwörter nur als Hash, rollen- und berechtigungsbasierte Zugriffskontrolle, wobei Meldungen der Meldestelle den von der Inhaberin oder dem Inhaber des Kontos des Verantwortlichen bestimmten Fallbearbeitenden vorbehalten sind und jeder Zugriff darauf protokolliert wird, ein nur fortschreibbares Protokoll der Änderungen an Personaldaten, befristeter und protokollierter Support-Zugriff, tägliche Sicherungen der Datenbanken, Ereignisprotokollierung.

Der aktuelle vollständige Text ist jederzeit unter <https://people.omegasuiteapp.com/legal/dpa?lang=de> abrufbar. Bei Fragen: amministrazione@outlinedigital.it.