Regelung zur Auftragsdatenverarbeitung

Diese Regelung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Vertragsverhältnis von Vertec mit dem Kunden ergeben. Massgebend sind insbesondere die folgenden gesetzlichen Bestimmungen: a) Für Kunden in Deutschland, Österreich und anderen Ländern der Europäischen Union: die DSGVO; b) für Kunden in der Schweiz: das schweizerische Datenschutzgesetz (DSG), die Verordnung zum Datenschutzgesetz (VDSG) sowie gegebenenfalls zusätzlich ebenfalls die DSGVO; c) für Kunden im Vereinigten Königreich: die Datenschutz-Grundverordnung des Vereinigten Königreichs (UK GDPR) und das Datenschutzgesetz 2018. Diese Regelung findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen durch Vertec personenbezogene Daten ("Daten") des Kunden verarbeitet werden.

1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Die Laufzeit dieser Regelung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Regelung nicht darüberhinausgehende Verpflichtungen ergeben.

Vertec verarbeitet personenbezogene Daten des Kunden als Auftragsdatenverarbeiter in den folgenden Fällen:

- Bei der Migration von Daten aus externen Systemen nach Vertec gemäss einem Kundenauftrag. In diesem Fall werden personenbezogene Daten nur soweit verarbeitet, wie der Kunde diese zur Migration nach Vertec vorsieht und an Vertec anliefert (z.B. Personendaten über Mitarbeitende des Kunden);
- Bei einem Auftrag zur Aufbewahrung einer Kopie der Vertec Datenbank (dies erfordert einen separaten Auftrag des Kunden) zu Test- oder Supportzwecken. In diesem Fall werden personenbezogene Daten bearbeitet, die durch den Kunden in der Vertec Datenbank gespeichert wurden (z.B. Personendaten über Mitarbeitende des Kunden);
- Beim Vertec Cloud Abo, bei dem Vertec im Kundenauftrag die Vertec Software betreibt, werden personenbezogene Daten bearbeitet, die durch den Kunden in der Vertec Datenbank gespeichert werden (z.B. Personendaten über Mitarbeitende des Kunden). Die Art der verarbeiteten personenbezogenen Daten hängt von der Nutzung der Software durch den Kunden ab und kann alle Kategorien personenbezogener Daten umfassen. Typischerweise betrifft das die nachfolgenden Kategorien.

  Kategorien personenbezogener Daten, z.B.

  - Stammdaten (z. B. Name, Adresse)
  - Kontaktdaten (E-Mail, Telefonnummer)
  - Inhaltsdaten (z. B. Texteingaben, Dokumente, Uploads)

  Kategorien betroffener Personen, z.B.

  - Kunden des Auftraggebers
  - Mitarbeiter des Auftraggebers
  - Interessenten
  - Sonstige Dritte, deren Daten durch den Kunden verarbeitet werden

  Welche personenbezogenen Daten konkret verarbeitet werden, liegt in der Verantwortung des Kunden, der diese Daten in Vertec speichert;
- Bei der Nutzung des Vertec Service für die optionale Belegerkennung von Spesen- und Kreditorenbelegen. Mit diesem Service hat der Kunde die Möglichkeit, kommerzielle Daten mittels eines AI-basierten Service aus Bild- oder PDF-Dateien zu extrahieren, um sie mit Vertec zu verarbeiten. Zwar werden mit dem Service weder der Input (Spesen- und Kreditorenbelege) noch der extrahierte Output (kommerzielle Daten) dauerhaft gespeichert, jedoch wird die Identität des Kunden zur Kontrolle an den Service übermittelt. Zudem kann es sein, dass im Fehlerfall Bild- oder PDF-Dateien oder der extrahierte Output in Logfiles abgespeichert werden. Eine dauerhafte Verknüpfung solcher Daten zur Identität des Kunden erfolgt jedoch nicht.
- Bei der Nutzung des optionalen AI Know-how Management Moduls. Dies ist ein als Cloud Dienst bereitgestellter, AI basierter Chat der auf den Vertec Daten beruht. Die für den Chat relevanten Daten, vor allem Aktivitäten und Dokumente, aber auch Stammdaten von Adressen und Projekten/Mandaten, unter Umständen auch Personendaten, werden in eine von Vertec betriebene Datenbank gespeichert und indiziert. Bei einer Anfrage via Vertec AI Chat werden für die Frage relevante Daten aus dem Index geholt und dem durch den Kunden vorkonfigurierten LLM geschickt für die Antworterstellung.

2 Anwendungsbereich und Verantwortlichkeit

Vertec verarbeitet personenbezogene Daten im Auftrag des Kunden und nach seinen Weisungen. Der Kunde ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Daten-

schutzgesetze für die Rechtmässigkeit der Datenverarbeitung verantwortlich ("Verantwortlicher" im Sinne des Art. 4 Nr. 7 DSGVO resp. Art. 5 lit. j. DSG).

Die Weisungen werden durch den Vertrag festgelegt. Weisungen des Kunden, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt und sind kostenpflichtig.

3 Pflichten von Vertec

Vertec darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Kunden verarbeiten, ausser es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor oder ein Rechtfertigungsgrund gemäss Art. 9 Abs. 4 DSG. Vertec informiert den Kunden unverzüglich, wenn Vertec der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstösst. Vertec darf die Umsetzung der Weisung solange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde.

Vertec wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Vertec wird technische und organisatorische Massnahmen zum angemessenen Schutz der Daten des Kunden treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DSGVO) resp. des DSG (Art. 8 DSG) genügen. Sie müssen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Die entsprechenden Prozesse sowie die eingeführten technischen und organisatorischen Massnahmen in Bezug auf den Datenschutz werden im Rahmen der ISO 27001 (Informationssicherheit) und ISO 9001 Zertifizierung (Qualitätsmanagement) von externen Auditoren bewertet und geprüft. Von den technischen und organisatorischen Massnahmen, die von der ISO 27001 im normativen Anhang A vorgesehen sind ("Referenzmassnahmenziele und –massnahmen", englisch "Controls") und im Kontext des Abschnittes 6.1.3 angewendet werden, bestätigt Vertec in der "Erklärung zur Anwendbarkeit" ("Statement of Applicability") die Anwendbarkeit allen Controls. Die Anwendung der Referenzmassnahmenziele und –massnahmen im Rahmen der ISO 27001 Norm wird ebenfalls von externen Auditoren bewertet und zertifiziert. Vertec wird den Kunden in geeigneter Form informieren, falls ihm die Zertifikate in Zukunft abgesprochen würden, und händigt ihm auf Wunsch Kopien dieser aus.

Vertec unterstützt soweit vereinbart und gegen gesonderte Vergütung den Kunden im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche von betroffenen Personen gem. Kapitel III der DSGVO resp. gem. dem 4. Kapitel des DSG sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO resp. Art. 24 DSG und 25 DSG genannten Pflichten.

Vertec gewährleistet, dass es den mit der Verarbeitung der Daten des Kunden befassten Mitarbeitern und andere für Vertec tätigen Personen untersagt ist, die Daten ausserhalb der Weisung zu verarbeiten. Ferner gewährleistet Vertec, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

Vertec unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt werden. Vertec trifft die erforderlichen Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Kunden ab.

Vertec nennt dem Kunden den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Vertec gewährleistet, ihre Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO resp. Art. 1 ff. VDSG nachzukommen, ein Verfahren zur regelmässigen Überprüfung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

Vertec berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Kunde dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt Vertec die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Kunden oder gibt diese Datenträger an den Kunden zurück. Diese Leistungen sind gesondert zu vergüten.

Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Kunden entweder herauszugeben oder zu löschen.

Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO resp. gemäss den anwendbaren Bestimmungen des schweizerischen Rechts, verpflichtet sich Vertec den Kunden bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen. Diese Leistungen sind gesondert zu vergüten.

4 Pflichten des Kunden

Der Kunde hat Vertec unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO resp. nach den anwendbaren Bestimmungen des schweizerischen Rechts gilt Abschnitt 3 Abs. 10 dieses Dokumentes entsprechend.

Der Kunde nennt Vertec den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an Vertec, wird Vertec die betroffene Person an den Kunden verweisen. Vertec leitet den Antrag der betroffenen Person unverzüglich an den Kunden weiter. Vertec haftet nicht, wenn das Ersuchen der betroffenen Person vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6 Nachweismöglichkeiten

Vertec weist dem Kunden auf Aufforderung die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

Sollten im Einzelfall Inspektionen durch den Kunden erforderlich sein, muss der Kunde dafür einen anerkannten Datenschutzexperten beauftragen. Die Prüfung durch den Datenschutzexperten ist zu den üblichen Geschäftszeiten durchzuführen unter Berücksichtigung einer angemessenen Vorlaufzeit. Vertec darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Massnahmen abhängig machen. Sollte der durch den Kunden beauftragte Prüfer in einem Wettbewerbsverhältnis zu Vertec stehen, hat Vertec gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf Vertec eine Vergütung verlangen.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Kunden eine Inspektion vornehmen, gilt grundsätzlich der vorherige Absatz entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt.

7 Subunternehmer (weitere Auftragsverarbeiter)

Der Einsatz von Subunternehmern, ausgenommen Gruppengesellschaften von Vertec, als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Kunde vorher zugestimmt hat.

Ausgenommen davon ist die Verarbeitung von Daten im Rahmen des Vertec Cloud Abos und weiterer optionalen Cloud Dienste, für welches der Kunde die Zustimmung zum Einsatz von Subunternehmern mit Vertragsabschluss erteilt.

Vertec arbeitet diesbezüglich mit Subunternehmern zusammen, welche hier aufgeführt sind: https://www.vertec.com/ch/agb/subliefe-ranten/.

Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn Vertec weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Vertec wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmassnahmen zu gewährleisten.

Erteilt Vertec Aufträge an Subunternehmer, so obliegt es Vertec, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

Vertec ist berechtigt, ohne die explizite Zustimmung des Kunden die Subunternehmer auszutauschen, falls die neuen Subunternehmer ein gleiches oder höheres Niveau an Datenschutz gewährleisten. Über entsprechende Änderungen informiert Vertec auf ihrer Website (siehe Link oben) sowie über den E-Mail-Newsletter (Anmeldung erforderlich). Widerspricht der Kunde einer solchen Änderung, steht ihm hinsichtlich der betroffenen Cloud Dienste ein ausserordentliches Kündigungsrecht zu.

8 Informationspflichten, Schriftformklausel, Rechtswahl

Sollten die Daten des Kunden bei Vertec durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat Vertec den Kunden unverzüglich darüber zu informieren. Vertec wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschliesslich beim Kunden liegen.

Änderungen und Ergänzungen dieser Regelung und aller ihrer Bestandteile – einschliesslich etwaiger Zusicherungen Vertecs – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Bei etwaigen Widersprüchen gehen Regelungen des Vertrages dieser Regelung zum Datenschutz vor. Sollten einzelne Teile dieser Regelung unwirksam sein, so berührt dies die Wirksamkeit der Regelung im Übrigen nicht.

Es gilt das Recht des Vertrages.

9 Haftung und Schadenersatz

Der Kunde und Vertec haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung respektive entsprechend den anwendbaren Bestimmungen des schweizerischen Rechts.

Übersicht über technische und organisatorische Massnahmen

10 Grundsätze, IT Grundschutz

Das Informationssicherheits-Managementsystem der Vertec misst dem Schutz der IT Infrastruktur und der Ausbildung und Bewusstseinsbildung der Mitarbeitenden bez. den Bedrohungen der Informationssicherheit eine hohe Bedeutung zu.

Den folgenden Themenblöcken wird dabei eine erhöhte Wichtigkeit beigemessen:

- Schutz der Client-Infrastruktur. Eine grosse Bedrohung für die Informationssicherheit geht von Arbeitsplatzrechnern und Laptops der Mitarbeitenden aus. Dem Schutz dieser Infrastruktur misst Vertec einen sehr hohen Stellenwert bei. Schutzmassnahmen beinhalten u. a.: Virenscanner, Verschlüsselung der Harddisks, Patchmanagement-Systeme, Härtung der Systeme gegen Angriffe über unnötig offene Ports. Zum Schutz der Client-Infrastruktur gehört auch Förderung des Bewusstseins der Belegschaft bez. den Risiken bez. Malware und Social Engineering.
- Trennung der Netze: die internen Netze der Vertec sind getrennt von Netzen mit Kundendiensten. Auch einzelne kundenbezogenen Dienste sind untereinander nur wo absolut nötig verbunden (z.B. nutzt das Forum das Kundenportal, damit sich Kunden am Forum anmelden können).
- Administrativer Zugriff auf Serverressourcen ist stark eingeschränkt auf ein kleines Team von IT-Administratoren.
- Sämtliche vorhandenen Passwörter sind nach dem "need to know" Prinzip nur für diejenigen Benutzer verfügbar, welche im entsprechenden Prozess mitarbeiten.
- Physische Sicherheit an den Vertec Standorten. Büroräumlichkeiten sind permanent verschlossen. Zugang zu den internen Serverräumlichkeiten ist via Panzertür und Codeschloss geschützt.
- Umgang mit Kundendaten (Daten im Besitz von Kunden, nicht nur, aber auch, Personendaten). In einem etablierten monatlichen Prozess werden Kundendaten (z.B. aus Supportanfragen) identifiziert und gelöscht, falls diese nicht mehr für einen Auftrag benötigt werden und falls kein Auftrag zur Speicherung einer Vertec Datenbank vorliegt.
- Der Zugriff zum Vertec LAN ist eingeschränkt für Geräte die gemäss Abschnitt 10 geschützt sind. Fremde Geräte sind hardwaremässig vom Zugriff auf das interne LAN ausgeschlossen (kein "BYOD").

11 Verarbeitung von Personendaten im internen Vertec Netzwerk

Bei einem Auftrag zur Migration von Daten oder einem Auftrag zur Speicherung einer Vertec Datenbank erfolgt die Verarbeitung auf einem Server mit eingeschränktem Zugriff. Alternativ dazu kann die Migration von Daten auch auf der Infrastruktur des Kunden erfolgen.

Nach Beendigung des Auftrages löscht Vertec die Kundendaten.

12 Vertec Cloud Abo

Mit dem Vertec Cloud Abo wird die Vertec Software von Vertec betrieben. Welche (und ob überhaupt) Personendaten mit Vertec verarbeitet werden, hängt vom konkreten Anwendungsfall des Kunden ab. Vertec verarbeitet die Personendaten des Kunden da in der Regel vollständig automatisch, eine manuelle Bearbeitung oder sogar Anreicherung erfolgt dabei nicht.

Ausnahmen sind:

- Kontrolle der Funktionsweise des Backup-Systems der Vertec Datenbank durch ein Restore im Stichprobenverfahren.
- Bei einem Auftrag des Kunden zur Auslieferung der Vertec Datenbank oder einem Auftrag des Kunden zum Restore.
- Im Disaster Recovery Fall
- Für Testzwecke

Die Cloud Abo Infrastruktur besteht aus mehreren verbundenen Linux und Windows Servern an den Cloud Abo Standorten Schweiz, Deutschland und Österreich. Der administrative Zugriff ist auf diese Server vom Personenkreis her stark eingeschränkt. Die Kommunikation zwischen den Standorten und den Servern untereinander, von der Cloud Abo Infrastruktur zu den Client-Applikationen der Kunden sowie der administrative Zugriff, erfolgt verschlüsselt.

Vertec erstellt jede Nacht ein Backup von allen Vertec Cloud Abo Instanzen der Kunden und speichert diese auch bei Backupdienstleistern (siehe Abschnitt 7).

Vertec prüft die Availability der Infrastruktur via einen externen Dienst, welcher aber keinen Zugriff auf Kundendaten hat.