Regelung zur Auftragsdatenverarbeitung

Diese Regelung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, insbesondere der DSGVO, die sich aus dem Vertragsverhältnis von Vertec mit dem Kunden ergeben. Sie 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, und beim Vertec Webaccess Service, bei dem Vertec die Connectivity zur Verfügung stellt. In diesem Fall werden personenbezogene Daten bearbeitet, die durch den Kunden in der Vertec Datenbank gespeichert werden (z.B. Personendaten über Mitarbeitende des Kunden);

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 Datenschutzgesetze für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ("Verantwortlicher" im Sinne des Art.4 Nr. 7 DSGVO).
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. 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) 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 27001:2013 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 von 113 der total 114 vorgesehenen Controls. Einzig bei Control A.11.1.6 ist die Anwendbarkeit nicht gegeben. 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 sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO 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 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, 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, 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 dem Vertec Webaccess Service, für welche der Kunde die Zustimmung zum Einsatz von Subunternehmern mit Vertragsabschluss erteilt.
Vertec arbeitet diesbezüglich mit folgenden Subunternehmern zusammen:

- CLOUDSIGMA Holding AG, CLOUDSIGMA AG (beide Schweiz) und CLOUDSIGMA Germany GmbH (Deutschland) für Rechenzentrumsleistungen als IaaS Provider an den Cloud Abo Standorten Zürich und Frankfurt. Das Informationssicherheits-Managementsystem Cloud Sigma ist ebenfalls nach ISO 27001 zertifiziert.
- Akenes SA (Exoscale), 1006 Lausanne, Schweiz für Rechenzentrumsleistungen als IaaS Provider am Cloud Abo Standort Zürich. Das Informationssicherheits-Managementsystem Akenes SA ist ebenfalls nach ISO 27001 zertifiziert.
- appGenerics GmbH, 90552 Röthenbach a.d. Pegnitz, Deutschland für die Entwicklung des Vertec Kundenportals und für die Entwicklung von Verwaltungssoftware für das Vertec Cloud Abo.
- netnea AG, 3097 Liebefeld, Schweiz für den Betrieb der Vertec Cloud Services.
- Infomaniak Network SA, 1227 Les Acacias, Schweiz für Backups der Vertec Cloud Abos. Das Informationssicherheits-Managementsystem Infomaniak Network SA ist ebenfalls nach ISO 27001 zertifiziert.

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.

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.

Übersicht über technische und organisatorische Maßnahmen

10 1 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. Anmeldung zum Testzugang auf das Cloud Abo via Vertec Kundenportal).
- 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 und wo nötig wurde der Einbruchschutz (z.B. Fenster) verstärkt. 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.

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 im internen Netzwerk der Vertec (LAN). Alternativ dazu kann die Migration von Daten auch auf der Infrastruktur des Kunden erfolgen.
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").
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, hängt vom konkreten Anwendungsfall des Kunden ab. Vertec verarbeitet die Personendaten des Kunden da in 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.

Die Cloud Abo Infrastruktur besteht aus mehreren verbundenen Linux und Windows Servern an den beiden Cloud Abo Standorten Zürich und Frankfurt. Der administrative Zugriff auf diese Server ist 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 bei einem Backupdienstleister (siehe Abschnitt 7).

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