Zwischen dem seventhings Kunden (Auftraggeber) und der seventhings GmbH (Auftragnehmer) wird nachfolgender Vertrag geschlossen.

Präambel

(1) Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Nutzung gemäß §1 Absatz 2 in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Vertrags. Eine Kündigung des Vertrages bewirkt automatisch die Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

§ 1 Gegenstand, Dauer und Spezifizierung des Auftrags

(1) Die Nutzung der Software SEVENTHINGS erfolgt als SaaS-Lösungen (Cloud) auf den Servern des Auftragnehmers. Gegenstand und Laufzeit dieser Vereinbarung ist im Vertrag definiert. Für die Beurteilung der Zulässigkeit der Datenerhebung / -verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsdatenverarbeitung der Nutzung der Software SEVENTHINGS ergeben. Die Erhebung bzw. Verarbeitung oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung im Zusammenhang mit der Erbringung von Servicedienstleistungen für die Software SEVENTHINGS.

(2) Produktbeschreibung:
Wir helfen Unternehmen den hohen Aufwand der manuellen Inventarisierung von Mobiliar, IT-Equipment, Maschinen, etc. zu beseitigen, indem wir die Inventarverwaltung digitalisieren und automatisieren. Das Inventar wird mit maschinenlesbaren Etiketten versehen (Barcode, QR-Code oder RFID-Tag). Bei der Inventur werden die Etiketten mit einem mobilen Datenerfassungsgerät (Smartphone, Industriescanner oder RFID Reader) in Verbindung mit der App SEVENTHINGS MDT oder App SEVENTHINGS Smartphone gescannt und zum Datenbestand hinzugefügt. Damit schaffen wir einen einfachen Überblick über alle Gegenstände (Inventare) im Unternehmen. Die geprüften Inventurdaten können dann aus der Software SEVENTHINGS direkt in bestehende Dritt-System übertragen werden. Der Inventarverantwortliche erhält über seinen Zugang einen aktuellen Soll-Ist-Vergleich und kann auftretende Abweichungen selbst in der Software SEVENTHINGS bearbeiten. Änderungs- und Abgangsprotokolle sind nicht mehr nötig.

(3) Kreis der Betroffenen können u.a. sein,

☒ Persona; Beschäftigte einschließlich Freiwilliger, Beauftragte, Zeitarbeitskräfte und Aushilfen
☒ Studenten und Schüler

(4) Diese Vereinbarung regelt die Maßnahmen, die Art. 28 DS-GVO zwischen Auftraggeber und Auftragnehmer zum Schutz personenbezogener Daten verlangt.

Art der Auftraggeber-Daten	Arten der Verarbeitung	Gegenstand und Zweck der Verarbeitung	Kreis der Betroffenen
Name, Vorname Technische Daten zu Geräten mit ggf. Personenbezug, E-Mail-Adresse, Standort Private Anschrift und E-Mail	Zuordnung zum jeweiligen Inventar/ Gegenstand Angebot und Verkauf von Inventar	Bereitstellung einer Software zur Inventarisierung als SAAS-Lösung. Gegeben falls Datenmigration und Bereitstellung des Modul Circularity Hub für Angebote zum Verkauf von Inventar.	Auftraggeber/ Mitarbeiter

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet ggf. personenbezogene Daten im Auftrag des Auftraggebers gemäß dem Vertrag und dessen Leistungsbeschreibung und wie in dieser Vereinbarung konkretisiert. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

(2) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung. Sollte eine Ausnahme des Art. 28 Abs. 3 lit. a DSGVO vorliegen, informiert der Auftragnehmer den Auftraggeber umgehend.

(3) Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Die begründeten Kosten sind durch den Auftraggeber zu tragen. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Weisungsempfänger beim Auftragnehmer sind:

- Die beauftragende Fachabteilung oder Einzelpersonen:
  Customer Success Management (CSM)
- (bzw. separat benannter Stellvertreter/Nachfolger)
  Steffen Prasse

§ 3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer wird die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung dokumentieren und dem Auftraggeber zur Prüfung übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragnehmer wird die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herstellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. [Einzelheiten in Anlagen 2].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit wird der Auftragnehmer ggf. alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

§ 4 Pflichten des Auftragnehmers und Qualitätssicherung

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

b) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

c) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlagen 2]. Zur der Unterstützung des Auftraggebers gemäß Art. 28 Abs. 3 lit. e, 32 DS-GVO, existieren die notwendigen Maßnahmen.

e) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) Der Auftraggeber wird über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, informiert.

g) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, wird ihn der Auftragnehmer unterstützen.

h) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet, wird.

i) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit wird der Auftragnehmer ggf. alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

§5 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer wird die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers– auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, berichtigen, löschen oder deren Verarbeitung einschränken. Angesichts der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.

(2) Soweit vom Leistungsumfang umfasst, werden Löschkonzepte, Rechte auf Vergessenwerden, Berichtigungen, Daten Portabilität und Auskünfte nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sichergestellt.

§6 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer verpflichtet sich, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Sämtliche vertraglichen Regelungen in der Vertragskette werden auch jedem weiteren Unterauftragnehmer auferlegt.

(2) Der Auftragnehmer wird Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftragnehmer wird die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers– auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeiten, berichtigen, löschen oder deren Verarbeitung einschränken. Angesichts der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.

(3) Beauftragt der Auftragnehmer einen Unterauftragnehmer mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Auftraggebers), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsnehmer gemäß dieser Vereinbarung gelten. Der Auftragnehmer stellt sicher, dass der Unterauftragnehmer die Pflichten erfüllt, denen der Auftragsnehmer entsprechend diesen Vereinbarung und gemäß der DSGVO unterliegt.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden werden erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung vollzogen.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(6) Die Verarbeitung personenbezogener Daten durch Unterauftragnehmer in einem Drittland ist grundsätzlich unzulässig. Wird die Verarbeitung personenbezogener Daten in besonderen Ausnahmefällen und nach vorheriger Freigabe durch den Auftraggeber in einem Drittland vorgenommen, dann darf dies nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Des weiteren erfolgt diese ausschließlich unter Zugrundelegung der Standardvertragsklauseln für Auftragsverarbeiter in Form des Durchführungsbeschluss (EU) 2021/914 für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind. Der für die Datenverarbeitung verantwortliche Auftraggeber gilt dabei als Datenexporteur, der im Drittland ansässige Unterauftragnehmer als Datenimporteur.

(7) Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 7 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der einschlägigen Datenschutzgesetze, insbesondere bezogen auf die Verpflichtungen als Auftraggeber für die Rechtmäßigkeit der Vergabe der Verarbeitung personenbezogener Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich.

(2) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeiteten Daten ein angemessenes Schutzniveau bieten.

(3) Die Weisungen werden anfänglich durch den Vertrag und diese Vereinbarung festgelegt und können vom Auftraggeber in schriftlicher Form oder Textform an, die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (sogenannte Einzelweisung). Änderungen des Verarbeitungsgegenstandes oder Verfahrensänderungen sind gemeinsam abzustimmen und entsprechend Satz 1 schriftlich oder in Textform vom Auftraggeber festzulegen. Die letzte Entscheidungsbefugnis liegt beim Auftraggeber.

(4) Der Auftraggeber hat das Recht, insbesondere in folgendem Umfang zusätzliche Weisungen gegenüber dem Auftragnehmer zu erteilen:

☒ Im Hinblick auf die Erfüllung des Vertrages

☒ Im Hinblick auf zusätzlichen Datensicherungsmaßnahmen

☒ Im Hinblick auf das Vorgehen bei Datenschutzverstößen

(5) Der Auftragnehmer nennt dem Auftraggeber - auf Verlangen - den Ansprechpartner für die im Rahmen dieser Vereinbarung anfallende Datenschutzfragen.

(6) Für den Fall, dass sich die weisungsberechtigten Personen oder die primären Kontaktpersonen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich mitteilen.

(7) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(8) Im Falle einer Inanspruchnahme einer Vertragspartei durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO in Bezug auf die Datenverarbeitung nach dieser Vereinbarung oder in deren Zusammenhang, verpflichtet sich die in Anspruch genommene Vertragspartei, die andere Vertragspartei unverzüglich zu informieren. Die Vertragsparteien werden sich bei der Abwehr des Anspruchs gegenseitig unterstützen.

§ 8 Mitteilung bei Verstößen

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 9 Kontrollpflichten des Auftraggebers

Der Auftragnehmer stellt alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung und in Datenschutzrecht niedergelegten Pflichten zur Verfügung, ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt dazu bei.

Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und so dann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis.

- Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen.
- oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.
- Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen gemäß Art. 28 Abs. 3 S. 2 lit. h, 32 DS-GVO mitwirkt. Darüber hinaus gehende Mehraufwände sind durch den Auftraggeber zu tragen.

§10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber wird der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung kann vorgelegt werden.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, werden durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt.

§ 11 Sonstiges

(1) Für Nebenabreden ist die Schriftform erforderlich.

(2) Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(3) Es gilt deutsches Recht. Als Gerichtsstand wird Dresden vereinbart.

[Stand: März 2024]

Anlagen:
Anlage 1: Unterauftragnehmer
Anlage 2: Beschreibung der technischen und organisatorischen Maßnahmen zum Betrieb des Inventarmanagers
Anlage 3: Beschreibung der technischen und organisatorischen Maßnahmen der Telekom für den Betrieb des Rechenzentrums und der Sever-Hostings

Anlage 1 Unterauftragnehmer

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen
Open Telekom Cloud der Deutschen Telekom AG T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main	Infrastructure-as-a-Service, Hosting
TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen	Fernwartungen
Strato AG, Pascalstr. 10, 10587 Berlin	Infrastructure-as-a-Service, Hosting

Anlage 2 Beschreibung der technischen und organisatorischen Maßnahmen zum Betrieb des Inventarmanagers

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO):

Verantwortlicher:
seventhings GmbH
Hainstrasse 2, 01097 Dresden (Deutschland)

Gesetzlicher Vertreter:
Die Geschäftsführung

Datenschutzbeauftragter:
DataOrga® GmbH
E-Mail: dsb@seventhings.com

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:
- Siehe TOMs der Telekom

M.1.2 Beschreibung der Zugangskontrolle:
- Authentifikation mit Benutzer + Passwort - Authentifikation mit Benutzer + Passwort [umgesetzt]
- Benutzerberechtigungen - Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt) [umgesetzt]
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes [umgesetzt]
- MDM - Einsatz von Mobile Device Management [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]

M.1.3 Beschreibung der Zugriffskontrolle:
- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts [umgesetzt]
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit [umgesetzt]
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]

M.1.4 Beschreibung der Weitergabekontrolle:
- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet [umgesetzt]
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen [umgesetzt]

M.1.5 Beschreibung des Trennungsgebots:
- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig) [umgesetzt]
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem [umgesetzt]

M.1.6 Beschreibung der Pseudonymisierung:
- Es erfolgt keine Pseudonymisierung.

M.1.7 Beschreibung der Verschlüsselung:
- Speicherung - Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard) [umgesetzt]
- Übertragung - Verschlüsselte Datenübertragung (z.B. E-Mailverschlüsselung nach PGP oder S/Mime, VPN, verschlüsselte Internetverbindungen mittels TLS/SSL, Einsatz FTAPI - Datentransfertool) [umgesetzt]

M.1.8 Beschreibung der Datenträgerkontrolle:
- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern [umgesetzt]

M.1.9 Beschreibung der Benutzerkontrolle:
- Passwortvergabe - Schutz der Benutzeraccounts durch Passwörter [umgesetzt]
- Sperrung von Ex-Mitarbeiter - Sperren von Benutzeraccounts ausgeschiedener Mitarbeiter [umgesetzt]
- Zweifaktor-Authentifizierung - Authentifikation mit Benutzername / Passwort und einem zweiten Faktor (z.B. Hardwaretoken, SMS, FIDO2) [umgesetzt]

M.1.10 Beschreibung der Übertragungskontrolle:
- Protokollierung - Protokollierung aller Abruf- und Übermittlungsvorgänge [umgesetzt]

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten [umgesetzt]
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe. [umgesetzt]

M.2.2 Beschreibung der Datenintegrität:

- Datensicherungskonzept - Erstellen eines Backup- und Wiederherstellungskonzeptes [umgesetzt]

M.2.3 Beschreibung der Speicherkontrolle:

- Berechtigungskonzept - Festlegung von Berechtigungen in einem Berechtigungskonzept [umgesetzt]
- Need-to-Know Prinzip - Anzahl der Berechtigungen und Administratoren auf das Notwendigste reduziert
- Protokollierung - Anzahl der Berechtigungen und Administratoren auf das Notwendigste reduziert [umgesetzt]

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware
- Backup- und Recoverykonzept - Erstellen eines Backup- und Recoverykonzepts [umgesetzt]

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen [umgesetzt]

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten [umgesetzt]
- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) [umgesetzt]
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO. [umgesetzt]
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten [umgesetzt]

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Audits - Durchführung regelmäßiger interner Audits [umgesetzt]
- DSB - Benennung eines Datenschutzbeauftragten [umgesetzt]
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen. [umgesetzt]
- Schwachstellenanalysen - Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest) [umgesetzt]
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (audatis MANAGER) [umgesetzt]
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. audatis MANAGER) [umgesetzt]
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO [umgesetzt]

M.4.3 Beschreibung der Organisationskontrolle:

- Datenschutzbeauftragter - Ein Datenschutzbeauftragter ist benannt, gemeldet und seine Kontaktdaten sind veröffentlicht [umgesetzt]
- Dokumentation der Verarbeitung - Aller Verarbeitungstätigkeiten sind dokumentiert und werden regelmäßig überprüft [umgesetzt]
- Richtlinien - Es existieren verbindliche Richtlinien für den Umgang mit personenbezogenen Daten
- Sensibilisierung - Mitarbeiter werden regelmäßig zum Datenschutz sensibilisiert und geschult [umgesetzt]

Anlage 3 Beschreibung der technischen und organisatorischen Maßnahmen der Telekom für den Betrieb des Rechenzentrums und der Sever-Hostings

Hinweis: Alle Daten zum SEVENTHINGS Inventar-Manager liegen in der Open Telekom Cloud der Deutschen Telekom AG

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO):

Verantwortlicher:
seventhings GmbH
Hainstrasse 2, 01097 Dresden (Deutschland)

Gesetzlicher Vertreter:
Die Geschäftsführung

Datenschutzbeauftragter:
DataOrga® GmbH
E-Mail: dsb@seventhings.com

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Alarmanlage - Einsatz einer Alarmanlage (evtl. mit Meldung an Sicherheitsdienst) [umgesetzt]
- Besucherprotokollierung - Protokollierung der Besucher (z. B. Besucherbuch) [umgesetzt]
- Chipkarten - Chipkarten-/Transponder-Schließsystem [umgesetzt]
- Pförtner - Personenkontrolle beim Pförtner [umgesetzt]
- Schlüsselverwaltung - Schlüsselregelung mit Dokumentation der Schlüssel (z. B. Schlüsselbuch) [umgesetzt]
- Videoüberwachung - Videoüberwachung der Zugänge [umgesetzt]

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort - Authentifikation mit Benutzer + Passwort [umgesetzt]
- Benutzerberechtigungen - Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt) [umgesetzt]
- Firewall - Einsatz von Firewalls zum Schutz des Netzwerkes [umgesetzt]
- Sorgfältige Personalauswahl - Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]

M.1.3 Beschreibung der Zugriffskontrolle:

- Berechtigungskonzept - Erstellen und Einsatz eines Berechtigungskonzepts [umgesetzt]
- Passwortlichtlinien - Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit [umgesetzt]
- Verschlüsselung von Datenträgern - Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren [umgesetzt]

M.1.4 Beschreibung der Weitergabekontrolle:

- SSL / TLS Verschlüsselung - Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet [umgesetzt]
- VPN-Tunnel - Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen [umgesetzt]

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung - Logische Mandantentrennung (softwareseitig) [umgesetzt]
- Produktiv- und Testsystem - Trennung von Produktiv- und Testsystem [umgesetzt]

M.1.6 Beschreibung der Pseudonymisierung:

- Es erfolgt keine Pseudonymisierung

M.1.7 Beschreibung der Verschlüsselung:

- Speicherung - Verschlüsselte Datenspeicherung [umgesetzt]
- Übertragung - Verschlüsselte Datenübertragung (z.B. VPN, verschlüsselte Internetverbindungen mittels TLS/SSL, Datentransfertool) [umgesetzt]

M.1.8 Beschreibung der Datenträgerkontrolle:

- Sichere Aufbewahrung - Sichere Aufbewahrung von Datenträgern [umgesetzt]
- Vernichtung - Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399) [umgesetzt]
- Verschlüsselung - Verschlüsselung von Datenträgern [umgesetzt]

M.1.9 Beschreibung der Benutzerkontrolle:

- Passwortvergabe - Schutz der Benutzeraccounts durch Passwörter [umgesetzt]
- Sperrung von Ex-Mitarbeiter - Sperren von Benutzeraccounts ausgeschiedener Mitarbeiter [umgesetzt]
- Zweifaktor-Authentifizierung - Authentifikation mit Benutzername / Passwort und einem zweiten Faktor (z.B. Hardwaretoken, SMS, FIDO2) [umgesetzt]

M.1.10 Beschreibung der Übertragungskontrolle:

- Protokollierung - Protokollierung aller Abruf- und Übermittlungsvorgänge [umgesetzt]

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Personalisierte Benutzernamen - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) [umgesetzt]
- Protokollierung - Protokollierung der Eingabe, Änderung und Löschung von Daten [umgesetzt]
- Zugriffsrechte - Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe. [umgesetzt]

M.2.2 Beschreibung der Datenintegrität:

- Datensicherungskonzept - Erstellen eines Backup- und Wiederherstellungskonzeptes [umgesetzt]

M.2.3 Beschreibung der Speicherkontrolle:

- Berechtigungskonzept - Festlegung von Berechtigungen in einem Berechtigungskonzept [umgesetzt]
- Need-to-Know Prinzip - Anzahl der Berechtigungen und Administratoren auf das Notwendigste reduziert [umgesetzt]
- Protokollierung - Anzahl der Berechtigungen und Administratoren auf das Notwendigste reduziert [umgesetzt]

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Antivirensoftware - Einsatz von Antivirensoftware zum Schutz vor Malware [umgesetzt]
- Auslagerung Datensicherung - Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort [umgesetzt]
- Backup- und Recoverykonzept - Erstellen eines Backup- und Recoverykonzepts [umgesetzt]
- Brandmeldeanlagen - Feuer- und Rauchmeldeanlagen [umgesetzt]
- Feuerlöschgeräte - CO2 Feuerlöschgeräte in Serverräumen [umgesetzt]
- IT-Notfallplan - Erstellung und Anwendung von IT-Notfallplänen [umgesetzt]
- Klimaanlage - Klimaanlage in Serverräumen [umgesetzt]
- Redundante Datenhaltung - Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum) [umgesetzt]
- Schutzsteckdosenleisten - Schutzsteckdosenleisten in Serverräumen [umgesetzt]
- Temperaturüberwachung - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen [umgesetzt]
- Unterbrechungsfreie Stromversorgung - (USV) Unterbrechungsfreie Stromversorgung [umgesetzt]

M.3.2 Beschreibung der raschen Wiederherstellbarkeit:

- Datenwiederherstellungen - Regelmäßige und dokumentierte Datenwiederherstellungen [umgesetzt]
- Notfallpläne - IT-Notfallpläne und Wiederanlaufpläne [umgesetzt]

M.4 Weitere Maßnahmen zum Datenschutz

M.4.1 Beschreibung der Auftragskontrolle:

- Audits - Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten [umgesetzt]
- Auswahl - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) [umgesetzt]
- AV-Vertrag - Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO. [umgesetzt]
- Laufende Überprüfung - Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten [umgesetzt]

M.4.2 Beschreibung des Managementsystems zum Datenschutz:

- Audits - Durchführung regelmäßiger interner Audits [umgesetzt]
- DSB - Benennung eines Datenschutzbeauftragten [umgesetzt]
- Incident-Response-System - Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen [umgesetzt]
- Managementsystem Datenschutz - Managementsystem zum Datenschutz [umgesetzt]
- Managementsystem Informationssicherheit - Managementsystem zur Informationssicherheit ISO 27001 [umgesetzt]
- Schulung - Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen. [umgesetzt]
- Schwachstellenanalysen - Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest) [umgesetzt]
- Software Voreinstellungen - Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO) [umgesetzt]
- Softwaregestützte Tools - Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen. [umgesetzt]
- Verpflichtung - Verpflichtung auf die Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO [umgesetzt]

M.4.3 Beschreibung der Organisationskontrolle:

- Datenschutzbeauftragter - Ein Datenschutzbeauftragter ist benannt, gemeldet und seine Kontaktdaten sind veröffentlicht [umgesetzt]
- Dokumentation der Verarbeitung - Aller Verarbeitungstätigkeiten sind dokumentiert und werden regelmäßig überprüft [umgesetzt]
- Richtlinien - Es existieren verbindliche Richtlinien für den Umgang mit personenbezogenen Daten [umgesetzt]
- Sensibilisierung - Mitarbeiter werden regelmäßig zum Datenschutz sensibilisiert und geschult [umgesetzt]