Zwischen dem seventhings Kunden (Auftraggeber) und der seventhings by ITEXIA 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	Zweck der Datenerhebung, -verarbeitung oder -nutzung	Kreis der Betroffenen
Name, Vorname Technische Daten zu Geräten mit ggf. Personenbezug, E-Mail-Adresse	Zuordnung zum jeweiligen Inventar/ Gegenstand	Der Auftragnehmer erbringt für den Auftraggeber Prüftätigkeiten, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann. Zur Authentifizierung und Berechtigung	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].

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 berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.

(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.

(3) Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer gemäß Anlage 1 unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

(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 Auftraggeber ermächtigt den Auftragnehmer, in seinem Namen (Auftraggeber) mit in Drittländern ansässigen Subunternehmen des Auftragnehmers einen Vertrag mit den Standardvertragsklauseln zu schließen. 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 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 mitwirkt. 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 – spätestens mit Beendigung der Leistungsvereinbarung – 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: Oktober 2022]

Anlagen:
Anlage 1 Unterauftragnehmer
Anlage 2 technisch organisatorische Maßnahmen - Basissicherheit

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

Anlage 2 Technisch organisatorische Maßnahmen – Basissicherheit

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

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☐ Alarmanlage ☐ Absicherung von Gebäudeschächten

- ☐ Automatisches Zugangskontrollsystem
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Schließsystem mit Codesperre
- ☒ Manuelles Schließsystem
- ☐ Biometrische Zugangssperren
- ☒ Videoüberwachung der Zugänge
- ☐ Lichtschranken / Bewegungsmelder
- ☒ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Personenkontrolle beim Empfang
- ☐ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☒ Zuordnung von Benutzerrechten
- ☐ Erstellen von Benutzerprofilen
- ☒ Passwortvergabe
- ☐ Authentifikation mit biometrischen Verfahren
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☐ Gehäuseverriegelungen
- ☒ Einsatz von VPN-Technologie
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☒ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Personenkontrolle beim Empfang
- ☐ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Tragepflicht von Berechtigungsausweisen
- ☐ Einsatz von Intrustion-Detection-Systemen
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☒ Einsatz von Anti-Viren-Software
- ☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
- ☒ Einsatz einer Hardware-Firewall
- ☒ Einsatz einer Software-Firewall

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☒ physische Löschung von Datenträgern vor Wiederverwendung
- ☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☒ Verschlüsselung von Datenträgern
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☐ Protokollierung der Vernichtung

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen, mtl. Logdatei
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☒ HTTPS gesicherte Fernwartungsverbindung

Regelung zur Fernwartung:
Fernwartung ist nur für vertraglich vereinbarte Wartungen entsprechend Servicevertrag zugelassen (On-Premises-Lösung). Die Fernwartung erfolgt mit Hilfe des Tools TeamViewer.
Die Fernwartung wird vom SEVENTHINGS Mitarbeiter dokumentiert (Wer, Wann, Dienstleister, Problemstellung und Ergebnis).

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☐ Vertragsstrafen bei Verstößen
- ☒ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust in der OTC der Telekom geschützt sind.

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Testen von Datenwiederherstellung
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ In Hochwassergebieten: Serverräume über der Wassergrenze
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Erstellen eines Notfallplans
- ☒ Serverräume nicht unter sanitären Anlagen
- ☒ OTC Deutsche Telekom

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Erstellung eines Berechtigungskonzepts
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☒ Festlegung von Datenbankrechten
- ☒ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☒ Trennung von Produktiv- und Testsystem