Auftragsverarbeitungs-Vertrag
nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

der

- Verantwortlichen (nachfolgend „**Auftraggeberin**" genannt) –

und der

LHM Services GmbH

mit Sitz in München, eingetragen im Handelsregister des Amtsgerichts München unter HRB 206063, Emmy-Noether-Straße 2, 80992 München, vertreten durch Herrn Martin Janke, Vorsitzender der Geschäftsführung

- Auftragsverarbeiter (nachfolgend „**Auftragnehmerin**" genannt) -

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Gegenstand der Verarbeitung

Die Auftragnehmerin erbringt umfangreiche technische und Service-Leistungen im Bereich Informations- und Kommunikationstechnik für Münchner Bildungseinrichtungen. Neben der Breitstellung von Hard- und Software sowie aller benötigten technischen Kommunikationsmittel gehört die Wartung und Betreuung der IT-Systeme, die Begleitung bei der Einführung neuer Technik mit maßgeschneiderten Schulungsangeboten für die Nutzer und der Betrieb sowie die kontinuierliche Weiterentwicklung der bereitgestellten IT-Services zum Leistungsumfang der Auftragnehmerin. Gegenstand der Auftragsverarbeitung sind die im Rahmen der Leistungserbringung der Auftragnehmerin verarbeiteten personenbezogenen Daten. Dieser Vertrag findet Anwendung auf alle Verarbeitungen personenbezogener Daten, die mit dem Auftrag in Zusammenhang stehen und bei denen die Auftragnehmerin oder durch sie beauftragte Dritte personenbezogenen Daten für die Auftraggeberin verarbeitet. Dies sind insbesondere Daten im Zusammenhang mit der Erbringung, Bereitstellung und Durchführung folgender Dienstleistungen

Server- und Client-Infrastruktur
IT-Infrastruktur für Schulungs- und Fortbildungszwecke
Digitale Präsentationsmedien
Outputmanagement

IuK-Managementsysteme
Telekommunikations-Infrastruktur
Netzwerk- und Kommunikationssysteme
Sicherheits-Systeme
Zugangssysteme
Applikationsmanagement
Architekturmanagement
Rechenzentrumsdienstleistungen

Die vorstehenden Dienstleistungen werden konkretisiert durch Anlage 1 zu diesem Vertrag.

1.2 Dauer der Verarbeitung

Der Vertrag beginnt mit dem Zeitpunkt der Bereitstellung der Dienste und wird auf unbefristete Dauer geschlossen. Er kann von beiden Vertragsparteien mit einer Frist von zwei Jahren zum Monatsende schriftlich gekündigt werden.
Darüber hinaus können die Vertragsparteien den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß einer Vertragspartei gegen diesen Vertrag vorliegt (außerordentliche Kündigung).

1.3. Art der verarbeiteten personenbezogenen Daten

Die Auftragnehmerin verarbeitet alle im Zusammenhang mit der Leistungserbringung der Auftragnehmerin stehenden personenbezogenen Daten. Hinsichtlich der Art und des Umfangs der verarbeiteten Daten wird auf die Anlage 2 zu § 46 BaySchO, bezüglich der Kategorien der verarbeiteten Daten insbesondere auf die Ziffern 3. der jeweiligen Abschnitte, verwiesen. Es werden insbesondere folgende Kategorien von personenbezogenen Daten verarbeitet:

Stammdaten (z.B. Namen, Geburtstag, Amtsbezeichnung),
Kontaktdaten (z.B. Anschrift, Telefon, Email-Adresse),
Log- und Protokolldaten (z.B. IP-Adresse, Datum Anmeldung, Dauer),
Angaben zum Dienst- / Beschäftigungsverhältnis (z.B. Besoldungsgruppe, Teilzeit),
Lehrbefähigung und -erlaubnis (z.B. Lehramt, Fächer),
unterrichtete Fächer (z.B. Stundenzahl, unterrichtete Fächer),
Stundenplan- und Vertretungsplandaten (z.B. Klasse, Fach, Präsenzstunden) ,
Gastschülereigenschaft (z.B. Status, Sprengel),
Schulwegdaten (z.B. Kostenfreiheit, benutzte Verkehrsmittel),
Unterrichtsdaten (z.B. Klasse, Ausbildungsrichtung, Sprachen),
Ausbildungs- und Praktikumsdaten (z.B. Ausbildungsdauer, -art),
Schullaufbahn (z.B. Einschulung, Wiederholungen),
Ein- und Austritt (z.B. Datum, Abschluss),
Leistungs- und Zeugnisdaten (z.B. Noten, Beurteilungen),
Absenzen (z.B. Dauer, Grund).

Die Auftragnehmerin verarbeitet besonders schützenswerte personenbezogene Daten gemäß Art. 9 DS-GVO, wie beispielsweise Gesundheitsdaten, Religionszugehörigkeit.

Im Rahmen der Erbringung der Dienstleistungen durch die Auftragnehmerin werden insbesondere personenbezogene Daten von folgenden betroffenen Personenkategorien verarbeitet:

- Schülerinnen, Schüler,
- Eltern, Personensorge- und Erziehungsberechtigte, Pflegeeltern etc.,
- Lehr-, Verwaltungs- und sonstiges Personal in den Einrichtungen,
- Mitarbeiter der Ausbildungsbetriebe,
- Dienstleister der Auftraggeberin

Hinsichtlich weiterer Details zu den verarbeiteten personenbezogenen Daten wird auf die jeweiligen Verzeichnisse von Verarbeitungstätigkeiten verwiesen.

2. Rechte und Pflichten der Auftragnehmerin

2.1 Die Auftragnehmerin verarbeitet Daten von betroffenen Personen ausschließlich im Rahmen der getroffenen Vereinbarungen und der dokumentierten Weisungen der Auftraggeberin sowie entsprechend den datenschutzrechtlichen Regelungen, sofern sie nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, verpflichtet ist. In letzteren Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO). Die Auftragnehmerin verwendet die zur Verarbeitung überlassenen Daten für keine anderen Zwecke und insbesondere nicht für eigene Zwecke. Kopien der Daten werden, ohne dass sie im Auftrag oder in diesem Vertrag geregelt sind, nicht erstellt.

2.2 Die Auftragnehmerin informiert die Auftraggeberin unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Ist die Rechtmäßigkeit einer Weisung zweifelhaft, ist die Auftragnehmerin berechtigt, die Durchführung der Weisung solange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird. Stehen schwere Persönlichkeitsrechtsverletzungen im Raum oder nimmt die Auftragnehmerin bei weisungsgemäßem Handeln das Risiko einer strafbaren Handlung auf sich, darf sie die Umsetzung der Weisung darüber hinaus aussetzen, bis die Parteien eine einvernehmliche Lösung gefunden haben.

2.3 Die Auftragnehmerin gestaltet ihre innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Sie trifft insbesondere geeignete technische und organisatorische Maßnahmen, um einen dem Risiko angemessenen Schutz der Daten der Auftraggeberin zu gewährleisten (Art. 32 Abs. 1 DSGVO). Sie trifft diese technischen und organisatorischen Maßnahmen so, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt sind. Die entsprechenden technischen und organisatorischen Maßnahmen ergeben sich aus der Anlage 2 zu diesem Vertrag in der jeweils gültigen Fassung. Änderungen der getroffenen Maßnahmen durch die Auftragnehmerin sind nur zulässig, wenn sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind der Auftraggeberin mitzuteilen und mit dieser abzustimmen. Die Auftragnehmerin dokumentiert die Umsetzung der in Anlage 2 zu diesem Vertrag festgelegten technischen und organisatorischen Maßnahmen.

2.4 Die Auftragnehmerin unterstützt die Auftraggeberin nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte (Art. 28 Abs. 3 Buchst. e DSGVO) und unterstützt die Auftraggeberin unter Berücksichtigung der ihr zur

Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

2.5 Die Auftragnehmerin gewährleistet, dass es den mit der Verarbeitung der Daten der Auftraggeberin befassten Beschäftigten und anderen für die Auftragnehmerin tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet die Auftragnehmerin, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

2.6 Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich, wenn ihr im Rahmen des Auftragsverhältnisses Verletzungen des Schutzes personenbezogener Daten der Auftraggeberin bekannt werden. Sie trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

2.7 Die Auftragnehmerin nennt der Auftraggeberin Ansprechpartner für im Rahmen des Vertrages anfallende Weisungen sowie einen etwaigen Datenschutzbeauftragten. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind der Auftraggeberin die Kontaktdaten eines neuen, zuständigen Ansprechpartners bzw. etwaigen Datenschutzbeauftragten unverzüglich anzuzeigen.

Ansprechpartner der Auftragnehmerin:

Sascha Königsberg, Leiter IT-Governance
UM-GO, Tel.: 089 620 980 530, Sascha.Koenigsberg@lhm-services.de

Datenschutzbeauftragte der Auftragnehmerin:

Birgit Steilen, Datenschutzbeauftragte
UM-GO, Tel.: 089 620 980 522, datenschutz@lhm-services.de

2.8 Die Auftragnehmerin berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn die Auftraggeberin dies anweist und dies vom Weisungsrahmen umfasst ist, es sei denn, die Weisung widerspricht etwaigen gesetzlichen Aufbewahrungspflichten.

2.9 Nach Auftragsende sind Daten, Datenträger sowie sonstige Materialien auf Verlangen und nach Wahl der Auftraggeberin entweder zurückzugeben oder zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur weiteren Speicherung der personenbezogenen Daten besteht.

2.10 Im Falle einer Inanspruchnahme der Auftraggeberin durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich die Auftragnehmerin, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen ihrer Möglichkeiten zu unterstützen.

3. Rechte und Pflichten der Auftraggeberin

3.1 Mit Übersendung der Annahmeerklärung nach Anlage 3 schließt die Auftraggeberin diesen Auftragsverarbeitungs-Vertrag als „Verantwortliche“ im Sinne des Art. 4 Nr. 7 DSGVO.

Die Auftraggeberin ist im Rahmen dieses Vertrags für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Beurteilung der Rechtmäßigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO, die Datenweitergabe an die Auftragnehmerin sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich.

3.2 Die Auftraggeberin informiert die Auftragnehmerin unverzüglich, falls sie in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.3 Im Falle einer Inanspruchnahme der Auftragnehmerin durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich die Auftraggeberin, die Auftragnehmerin bei der Abwehr der Ansprüche im Rahmen ihrer Möglichkeiten zu unterstützen.

3.4 Die Auftraggeberin benennt der Auftragnehmerin eine weisungsberechtigte Person und die/den Datenschutzbeauftragten in der Annahmeerklärung.

3.5 Die Auftraggeberin ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrags bestehen. Die Befugnisse der Aufsichtsbehörden – insbesondere nach Art. 58 Abs. 1 DSGVO – bleiben hiervon unberührt.

4. Anfragen betroffener Personen

Macht eine betroffene Person ihre Rechte gemäß Art. 15 ff. DSGVO gegenüber der Auftragnehmerin geltend, wird diese die betroffene Person an die Auftraggeberin verweisen, sofern eine Zuordnung an die Auftraggeberin auf Basis der Angaben der betroffenen Person möglich ist. Gemäß Nr. 2.4 dieses Vertrags unterstützt die Auftragnehmerin die Auftraggeberin nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen.

5. Kontrollrechte der Auftraggeberin

5.1 Die Auftragnehmerin stellt der Auftraggeberin alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 Satz 2 Buchst. h DSGVO).
5.2 Die Auftraggeberin ist berechtigt, sich vor Beginn und während der Verarbeitung von der Einhaltung der bei der Auftragnehmerin getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

5.3 Kontrollen vor Ort durch die Auftraggeberin oder durch einen, von dieser beauftragten, Prüfer erfolgen nur in Ausnahmefällen, wenn sich die Auftraggeberin ansonsten keinen hinreichenden Eindruck verschaffen kann. Die Kontrollen werden grundsätzlich nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlauffrist zu den üblichen Geschäftszeiten durchgeführt. Die Auftragnehmerin hat die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung abhängig zu machen, wenn die Möglichkeit besteht, dass die Auftraggeberin, oder der von dieser beauftragte Prüfer im

Rahmen seiner Inspektion auch Kenntnis von Daten erlangt, die die Auftragnehmerin im Auftrag eines anderen Verantwortlichen verarbeitet. Die Auftraggeberin stellt sicher, dass ein von ihr beauftragter Prüfer in keinem Wettbewerbsverhältnis zu der Auftragnehmerin steht.

6. Subunternehmer (weitere Auftragsverarbeiter)

6.1 Ein Subunternehmerverhältnis liegt vor, wenn die Auftragnehmerin weitere Auftragnehmer mit der ganzen oder einer Teilleistung der vereinbarten Leistung beauftragt. Die Auftragnehmerin trägt bei der Auswahl eines Subunternehmers insbesondere Sorge dafür, dass dieser hinreichende Garantien dafür bietet, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung personenbezogener Daten entsprechend den Anforderungen der Datenschutz-Grundverordnung erfolgt.
Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Leistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice (wenn ein Zugriff auf personenbezogene Daten des Auftraggebers ausgeschlossen ist), Reinigungskräfte und Prüfer. Die Auftragnehmerin trifft mit diesen Dritten im erforderlichen Umfang schriftliche Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten und behält sich Kontrollmaßnahmen vor, um den Schutz und die Sicherheit der Daten der Auftraggeberin zu gewährleisten.
Eine Verlagerung der Leistungen oder von Teilarbeiten dazu in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

6.2 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). In dem Vertrag mit dem Subunternehmer sind dieselben datenschutzrechtlichen Pflichten aus dem vorliegenden Vertrag dem Subunternehmer wirksam aufzuerlegen. Insbesondere muss die Auftraggeberin berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

6.3 Die Auftragnehmerin haftet gegenüber der Auftraggeberin für die Einhaltung der datenschutzrechtlichen Pflichten jenes Subunternehmers.

6.4 Die Auftraggeberin erteilt der Auftragnehmerin die allgemeine Genehmigung, weitere Auftragsverarbeiter (Subunternehmer) im Sinne des Art. 28 Abs.2 DS-GVO gemäß den vorgenannten Regelungen in Anspruch zu nehmen. Die Auftragnehmerin informiert die Auftraggeberin, wenn sie Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Die Auftraggeberin kann gegen derartige Änderungen Einspruch erheben.

6.5 Hinsichtlich weiterer Details, insbesondere hinsichtlich detaillierter Informationen zu bei Vertragsbeginn bestehenden Subunternehmern wird auf die jeweiligen Verzeichnisse von Verarbeitungstätigkeiten verwiesen.

7. Haftung und Schadensersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen

bzw. gegenüber betroffenen Personen gemäß Art. 82 DSGVO.

8. Schlussbestimmungen

8.1 Änderungen und Ergänzungen dieses Vertrags und aller ihrer Bestandteile – bedürfen einer schriftlichen abgefassten Vereinbarung, die den ausdrücklichen Hinweis darauf enthält, dass es sich um eine Änderung bzw. Ergänzung dieses Vertrags handelt.

8.2 Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so ist die Wirksamkeit der übrigen Regelungen hiervon nicht betroffen. In diesem Falle werden die Parteien einvernehmlich eine neue Regelung oder Ergänzung der bestehenden Regelung vereinbaren, die die unwirksame oder undurchführbare Regelung in einer Art und Weise ersetzt bzw. ergänzt, die der ursprünglich von den Parteien bei Abfassung dieser Anlage beabsichtigten Regelung am nächsten kommt, hätten sie denn die Unwirksamkeit oder Undurchführbarkeit bedacht. Dies gilt auch für Regelungslücken.

8.3 Dieser Vertrag lässt den „Grundsatzvertrag über IT- und TK-Leistungen an den Schulen, Kindertageseinrichtungen, Sportstätten und weiteren Einrichtungen im Zuständigkeitsbereich des Referats für Bildung und Sport der Landeshauptstadt München“ geschlossen zwischen der Landeshauptstadt München und der LHM Services GmbH, unberührt.

München 13.9.22

Ort Datum

LHM-Services GmbH

Anlage 1: Art und Umfang der Auftragsverarbeitung
Anlage 2: Technische und organisatorische Maßnahmen
Anlage 3: Annahmeerklärung

Anlage 1 zum Auftragsverarbeitungsvertrag

Art und Umfang der Auftragsverarbeitung

Server- und Client-Infrastruktur: Zentrale Beschaffung und Support von Server und Client-Hardware und -Software, gesteuerte und geplante Skalierbarkeit und Funktion im Rahmen der Fachanforderungen, Sicherstellung der Kompatibilität zu allen Systemen im Verbund sowie des Zugangs über Remote-Access-Technologien, Bereitstellung und Support von Medientechnik nach Fachanforderungen.

IT-Infrastruktur für Schulungs- und Fortbildungszwecke: Bereitstellung von IT Infrastruktur für Schulungsumgebungen (inkl. Applikationen, Test- und Schulungsdaten).

Digitale Präsentationsmedien: Präsentationsmedien sind Träger visueller und akustischer Information. Sie sind technische Hilfsmittel, die von ihren Inhalten unabhängig sind und mit unterschiedlichen Informationen genutzt werden können. Diese beziehen sich auf Klassenzimmer und Veranstaltungsbereiche (bspw. Aula, gemeinsame Mitte) und insbesondere auf Beamer, interaktive Whiteboards, Dokumentenkameras und zugehörige Audioanlagen für Beamer und interaktive Whiteboards.

Outputmanagement: Bereitstellung von Systemen zur Erfassung oder Ausgabe von Papierdokumenten, beispielsweise von Multifunktionsgeräten, zentrale Steuerung der Druckerinfrastruktur mit und ohne Scanfunktion und der dazugehörigen Betriebsmittelbeschaffung, sowie darüber hinaus Unterstützung bei der konzeptionellen Festlegung effizienter Druckerbereitstellung (lokale Drucker, Etagendrucker, etc.).

IuK-Managementsysteme: Einsatz übergreifender Softwarelösungen und Methoden zur zentralen Verwaltung und Steuerung der Client- und Serversysteme, kontrolliertes Software- und Patchmanagement, Inventarisierung, Installationsautomatismen und Asset-Management.

Telekommunikations-Infrastruktur: Zentrale verwaltete Telefonie- und Telefax-Dienste, inkl. Bereitstellung von Endgeräten und abgestimmter Hintergrundsysteme.

Netzwerk- und Kommunikationssysteme: Zentrale Bereitstellung von Netzwerk- und Kommunikationsdiensten zur Datenkommunikation, gesteuerte und geplante Skalierbarkeit und Funktion im Rahmen der Fachanforderungen, effizienter und anforderungsgerecht verfügbarer Betrieb von Netzwerkhintergrundsystemen zur Zugangssteuerung und generellem technischen Netzwerkmanagement sowie Planung, Einrichtung und Betrieb von Netzwerkinfrastruktur.

Sicherheits-Systeme: Zentrale und geschützte Systeme zur Erfüllung hoher Sicherheitsbedürfnisse bei Kommunikation (insbesondere beim Internetzugang), Virenschutz, Firewalls, Client-Sicherheit (Kontrolle der Schnittstellen, lokale Firewall, Festplattenverschlüsselung).

Zugangssysteme: Zutritts- oder Zugriffssteuerung nach Bedarf beispielsweise über RFID-Karten, Handvenenscanner oder intelligente Schließsysteme sowie Bereitstellung eines einheitlich gesteuerten Identitätsmanagements und Berechtigungswesens.

Applikationsmanagement: Kombinierte Entwicklung und Betreuung von Applikationen (Anwendungssoftware) über deren gesamten Lebenszyklus; dies beinhaltet auch die Anwenderbetreuung (Support) und die Weiterentwicklung der Software.

Architekturmanagement: Übergreifendes Festlegen von Systemarchitektur- und Technologiestandards zur Wahrung von Kompatibilitätsanforderungen und zur Sicherung eines effizienten Betriebs.

Rechenzentrumsdienstleistungen: Bereitstellung zertifizierter Rechenzentrumsinfrastruktur mit angemessener Ausfallsicherheit bis hin zu sehr hohen Sicherheitsanforderungen an verteilten Standorten.

Anlage 2 zum Auftragsverarbeitungsvertrag

Technische und organisatorische Maßnahmen

Entsprechend Art. 28 Abs. 1 DS-GVO in Verbindung mit Art. 32 DS-GVO sind die Vertragsparteien verpflichtet, die technischen und organisatorischen Maßnahmen festzulegen.

1. Maßnahmen zur Sicherung der Vertraulichkeit

1. 1 Zutrittskontrolle
Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren.

Beschreibung der Zutrittskontrollsysteme, wie z.B.:
Magnet- oder Chipkarten
Schlüssel mit dokumentierter Schlüsselausgabe
Türsicherungen (Sicherheitsschlösser, elektrischer Türöffner etc.)
Gesicherter Serverraum
Werkschutz/Pförtner/Empfang
Sorgfältige Auswahl von Reinigungspersonal

1.2 Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen können.

Beschreibung der Zugangskontrollsysteme, wie z.B.:
Kennwortverfahren (persönlicher und individueller User Log-In bei Anmeldung am System u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennwortes)
Login mit Benutzername und Passwort
Automatische Sperrmechanismen
Zwei-Faktor-Authentifizierung
Zuordnung von Benutzerrechten
Erstellen von Benutzerprofilen
Antiviren- und Spywarefilter
Verschlüsselung von Datenträgern

1.3 Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung der Zugriffskontrollsysteme, wie z.B.:

Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
Protokollierung von Zugriffen
Löschkonzepte

1.4 Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung der Trennungskontrollsysteme, wie z.B.:
Mandantenfähigkeit
Trennung von Produktiv- und Testsystemen
Physikalische Trennung von Systemen, Datenbanken, Datenträgern
Berechtigungskonzepte
Sandboxing

1.5 Pseudonymisierung
Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Beschreibung des Pseudonymisierungsverfahrens, wie z.B.:
Listenverfahren: Datensätze werden anhand einer Tabelle bestimmten Pseudonymen zugeordnet. Hierbei wird darauf geachtet, dass kein direkter Bezug zu den Daten hergestellt wird.
Berechnungsverfahren: Algorithmische Berechnung von Pseudonymen aus Identitätsdaten. Durch Anwendung eines kryptographischen Schlüssels wird gewährleistet, dass unbefugte Dritte aus den Identitätsdaten nicht das Pseudonym berechnen können.

2. Maßnahmen zur Sicherung der Integrität

2.1 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 sowie Maßnahmen, mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Beschreibung der Weitergabekontrolle, wie z.B.:
Verschlüsselung
Virtual Private Networks (VPN)

Sichere Transportbehälter

2.2 Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.
Beschreibung des Eingabekontrollverfahrens, wie z.B.:
Dokumentenmanagement

3. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle
Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wie z.B.:
Backup-Strategie
Unterbrechungsfreie Stromversorgung (USV)
Feuer- und Rauchmeldeanlagen
Klimaanlage in Serverräumen
Virenschutz
Firewall
Meldewege und Notfallpläne

3.2 Rasche Wiederherstellbarkeit
Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, wie z.B.:
Backup Konzept
Regelmäßige Tests der Wiederherstellung

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen, wie z.B.: Datenschutz-Management
Incident-Response-Management
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)