

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen dem/der

Leibniz-Institut für jüdische Geschichte und Kultur – Simon Dubnow e.V.

Goldschmidtstr. 28, 04103 Leipzig

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Auftragnehmer und Auftraggeber werden gemeinsam nachstehend auch Parteien genannt.

§ 1 Allgemeines

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten Art. 28 DSGVO als Dienstleister ausgewählt. Dieser Vertrag zur Auftragsverarbeitung (im Folgenden „Vertrag“) enthält nach dem Willen der Parteien den schriftlichen Auftrag zur Auftragsverarbeitung i. S. d. Art. 28 DSGVO und regelt die Rechte und Pflichten der Parteien.

Die Regelungen gelten unabhängig davon, ob zwischen den Vertragsparteien ein Leistungsvertrag abgeschlossen wurde. Die nachfolgenden Regelungen finden zudem auf alle Tätigkeiten des Auftragsverarbeiters Anwendung, die mit dem Leistungsvertrag im Zusammenhang stehen und bei denen Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter beauftragte weitere Auftragsverarbeiter (im Folgenden: Unterauftragsverarbeiter) mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

- (2) Es gelten die Begriffsbestimmungen des Art. 4 DSGVO.

§ 2 Gegenstand und Dauer des Auftrags

- (1) Der Gegenstand des Auftrags ergibt sich aus:
- a) ☒ dem Instandhaltungsvertrag **2024-DI-IT-VÜA-IV** für die Videoüberwachungsanlage des Dubnow-Instituts inklusive
 - Software-Reparaturen
 - Software-Updates bzw. Software-Pflege
 - ggf. Software-Anpassungen
 - b) ☐ einem Fernwartungs- bzw. Webconsultingvertrag
 - c) ☐ einem Systembetreuungsvertrag
 - d) ☐ einem ASP-/ Cloud Vertrag
 - e) ☐
 - f) ☐
- (2) Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.
- (3) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender zu vertretender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt.

§ 3 Konkretisierung des Auftragsinhalts

Der Auftragnehmer ist mit der fachlichen Plattformbetriebsführung der Anwendungen unter § 2 (1) beauftragt. Durch einen entsprechenden Wartungs- oder Nutzungsvertrag stellt er die benötigte Anwendungssoftware inkl. Softwareupdates zur Verfügung und wird im Supportfall mit der Fehlerbehebung beauftragt.

Der Auftraggeber ist und bleibt Verantwortlicher im datenschutzrechtlichen Sinne für die beim Auftragsverarbeiter vertragsgemäß und nach Weisung des Auftraggebers verarbeiteten Daten.

- (1) Die Verarbeitung der Daten erfolgt ausschließlich zum Zweck der fachlichen Betriebsführung, zur Bereitstellung der Anwendungssoftware und bei Supportanfragen. Das Recht einer Auswertung und Weiterverarbeitung der Daten obliegt allein dem Auftraggeber.
- (2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Abweichungen unter den Voraussetzungen der Art. 44, 45, 46, 47, 48, 49, 50 DSGVO bedürfen einer separaten Abrede in Schriftform.
- (3) Die Art der verarbeiteten personenbezogenen Daten und die Kategorien der von der Verarbeitung betroffenen Personen sind wie folgt festgelegt:

Art der Daten	Kategorien betroffener Personen
<input checked="" type="checkbox"/> Bildaufnahmen	<input checked="" type="checkbox"/> Geschäftsführung, Leitende Angestellte
<input checked="" type="checkbox"/> Personenstammdaten (insb. Name, Kennung, Kennzeichen)	<input checked="" type="checkbox"/> Beschäftigte des Auftraggebers
<input checked="" type="checkbox"/> Datums-, Zeit- und Zeitraumangaben	<input checked="" type="checkbox"/> Kunden des Auftraggebers
<input checked="" type="checkbox"/> Produkt-/Vertragsinteresse	<input checked="" type="checkbox"/> Interessenten des Auftraggebers
<input checked="" type="checkbox"/> Bewegungsdaten	<input checked="" type="checkbox"/> Lieferanten des Auftraggebers
<input checked="" type="checkbox"/> ggf. Kommunikationsdaten	<input checked="" type="checkbox"/> Abonnenten des Auftraggebers
<input type="checkbox"/>	<input checked="" type="checkbox"/> Handelsvertreter des Auftraggebers
	<input checked="" type="checkbox"/> Ansprechpartner des Auftraggebers
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>

§ 4 Technische und organisatorische Maßnahmen

- (4) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung und sodann regelmäßig, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren. Die Dokumentation ist dem Auftraggeber vor Auftragsdurchführung zur Prüfung zu übergeben. Die dokumentierten Maßnahmen gelten als akzeptiert und werden zur Grundlage des Auftrags, wenn der Auftraggeber nicht innerhalb einer Woche schriftliche Einwendungen gegenüber dem Auftraggeber erhebt. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (5) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere i. V. m. Art. 5 Abs. 1, 2 DSGVO herzustellen. Der Auftragnehmer ist dafür verantwortlich, die Datensicherheit und ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie der Belastbarkeit der Systeme durch geeignete Maßnahmen zu gewährleisten. Hierbei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die jeweilige Eintrittswahrscheinlichkeit und Schadenshöhe bezüglich der Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

- (6) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind durch den Auftragnehmer zu dokumentieren.

§ 5 Sicherstellung der Betroffenenrechte

- (1) Der Auftragnehmer berichtigt, löscht oder beschränkt die Nutzung von Daten des Auftraggebers nur auf dokumentierte Weisung eines Auftraggebers. Soweit sich eine betroffene Person bezüglich einer Berichtigung, Löschung oder Sperrung von Daten unmittelbar an den Auftragnehmer oder einen Dritten wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Soweit es vom vereinbarten Leistungsumfang umfasst ist, sind die Rechte auf Vergessen werden sowie auf Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer gegen angemessene Vergütung sicherzustellen.

§ 6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verpflichtet sich, ergänzend zu den Regelungen dieser Vereinbarung, die gesetzlichen Pflichten nach Art. 28, 29, 30, 31, 32, 33 DSGVO einzuhalten. Dies umfasst insbesondere:
- a) Die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 DSGVO ausüben kann. Dies gilt nur, soweit die gesetzliche Verpflichtung hierzu besteht. Die Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragnehmers hinterlegt.
 - b) Die Wahrung der Vertraulichkeit gem. Art. 28 Abs. 3 S. 2 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können bzw. bei denen ein Zugriff nicht ausgeschlossen werden kann, sind vor Aufnahme der auftragsbezogenen Handlungen auf das Datengeheimnis zu verpflichten und über die sich aus diesem Auftrag ergebenden besonderen Verschwiegenheitspflichten sowie die bestehende Weisungs- bzw. Zweckbindung zu belehren. Beides ist zu dokumentieren und auf Nachfrage nachzuweisen.
 - c) Zusammenarbeit mit dem Auftraggeber in Bezug auf Anfragen und Prüfungen von Aufsichts- oder Ermittlungsbehörden, soweit sich diese auf eine Verarbeitung beziehen, welche auf Grundlage oder im Zusammenhang mit diesem Vertrag erfolgt. Der Auftragnehmer informiert den Auftraggeber in diesen Fällen unverzüglich. Finden derartige Maßnahmen beim Auftraggeber statt, so sichert der Auftragnehmer seine Unterstützung gegen angemessene Vergütung zu.
- (2) Der Auftragnehmer prüft in regelmäßigen, mit dem Auftraggeber abzustimmenden Abständen die Einhaltung der getroffenen Vereinbarungen und der datenschutzrechtlichen Vorschriften, einschließlich seiner technischen und organisatorischen Maßnahmen und diesbezüglichen internen Prozesse, 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. Der Auftragnehmer protokolliert diese technischen und organisatorischen Maßnahmen sowie deren Prüfungen und legt die Berichte auf Nachfrage dem Auftraggeber vor.

§ 7 Geheimhaltungspflichten

- (1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen

ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

- (2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 8 Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart.

§ 9 Unterauftragsverhältnisse

- (1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann.

Der Auftraggeber stimmt der Beauftragung der in Anlage 2 unter der Bedingung des Abschlusses einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu,

- (2) Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
 - a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab per Mail oder in anderer Textform anzeigt und
 - b) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.
- (3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (4) 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.
- (5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (per Mail oder in anderer Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 10 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der beauftragte Prüfer ist von dem Auftragnehmer entsprechend zum Datengeheimnis und zur Verschwiegenheit zu verpflichten. Auf Verlangen ist die entsprechende Vereinbarung dem Auftragnehmer vorzulegen.

- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der vertraglichen Pflichten einschließlich der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
 - a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
 - b) das Bestehen unternehmerischer Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung;
 - c) die regelmäßige Durchführung von Selbstaudits;
 - d) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
 - e) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
 - f) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz);
 - g) individuelle Absprachen
- (4) Abs. (2) gilt für eine entsprechende Beauftragung eines externen Prüfers ebenso. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Ablehnungsrecht.
- (5) Abs. (2) gilt nicht, wenn der dringende Verdacht besteht, dass der Auftragnehmer wesentliche datenschutzrechtliche Pflichten verletzt.
- (6) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 11 Mitteilungs- und Unterstützungspflichten des Auftragnehmers

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32, 33, 34, 35, 36 der DSGVO 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 Verletzungseignissen ermöglichen.
 - b) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
 - c) Die Verpflichtung, dem 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-Folgeabschätzung.
 - e) Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf kein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 12 Weisungsbefugnis des Auftraggebers

- (1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich und mindestens in Textform.
- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.
- (3) Ansprechpartner (Namen / Funktion / Telefonnummer / Mail)
 - a) Weisungsbefugte Ansprechpartner des Auftraggebers sind:

Nicole Petermann / Verwaltungsleiterin / 0341-2173553 / petermann@dubnow.de
 - b) Ansprechpartner des Auftragnehmers sind:

§ 13 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 – hat der Auftragnehmer vorbehaltlich der Regelung in Absatz 3 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 ist auf Anforderung vorzulegen.
- (3) Unterlagen und Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 14 Haftung und Schadensersatz

- (1) Eine zwischen den Parteien in der Leistungsvereinbarung vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wird. Fehlt eine solche Haftungsregelung, so haftet der Auftragnehmer dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen nach den gesetzlichen Regelungen.
- (2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzvorschriften unzulässigen oder unrichtigen Verarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Verursachende gegenüber den Betroffenen verantwortlich.

§ 15 Schlussbestimmungen

- (1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse konkret gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen und den Gläubiger über die Tatsache zu informieren, dass es sich um Daten handelt, die im Auftrag verarbeitet werden.
- (2) Für Nebenabreden oder jegliche Art von Änderungen und Ergänzungen dieses Vertrages, einschließlich etwaiger Zusicherungen des Auftragnehmers, ist die Schriftform erforderlich. Dies gilt auch für einen etwaigen Verzicht auf das Schriftformerfordernis. Von der Schriftform kann durch ein elektronisches Format abgewichen werden (z.B. Email)
- (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor.
- (4) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht. In diesem Falle werden die Parteien eine der unwirksamen Regelungen wirtschaftlich möglichst nahekommende rechtswirksame Ersatzregelung treffen.

.....
(Ort/Datum)

.....
- Auftraggeber -

(Zeichnung in Textform:
Handelnder, Position)

.....
- Auftragnehmer -

(Zeichnung in Textform:
Handelnder, Position)

Anlage 1

Technisch-organisatorische Maßnahmen

§ 1 Gegenstand

Zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO) sichert der Auftragnehmer dem Auftraggeber das Vorhandensein der nachfolgenden technischen und organisatorischen Maßnahmen zu.

§ 2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

(1) Zutrittskontrolle

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen wie folgt verwehrt

- Schließsystem
- Personenkontrolle
- Auf Datenschutz verpflichtetes Reinigungspersonal

(2) Zugangskontrolle

Die unbefugte Nutzung der Datenverarbeitungssysteme wird durch folgende Maßnahmen verhindert:

- Benutzerkonto für jeden Mitarbeiter
- Zeitliche Zugangsbeschränkung
- Virenschutzlösungen
- Packet Filter Firewall
- Dedizierte Netze für sensible Systeme
- Authentifikation mit Passwort
- Schließsystem
- Personenkontrolle
- Auf Datenschutz verpflichtetes Reinigungspersonal

(3) Zugriffskontrolle

Nur Berechtigte können die ihnen freigegebenen personenbezogene Daten verarbeiten und nutzen, währenddessen Unbefugte diese Daten weder lesen noch verändern können. Dazu werden folgende Maßnahmen ergriffen:

- Dokumentiertes Berechtigungskonzept
- Rollenkonzept
- Differenzierte Berechtigungen für unterschiedliche Transaktionen/Funktionen
- Strenge Passwortrichtlinien
- Protokollierung der Anmeldevorgänge
- Aufteilung der Administratorrechte unter verschiedenen Personen
- Sicheres Löschen von Datenträgern
- Regelmäßige Passwortwechsel
- Protokollierung der Datenzugriffe

(4) Trennungskontrolle

Die Gewährleistung der getrennten Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten wird durch folgende Maßnahmen sichergestellt

- Differenzierte Berechtigungen bei der Datenverwaltung
- Logische Mandantentrennung
- Trennung von Produktiv- und Testsystem
- Differenzierung administrativer Aufgaben bei der Datenverwaltung

(5) Pseudonymisierung

Personenbezogene Daten werden in einer Weise verarbeitet, dass sie ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, es sei denn, ein Personenbezug ist zwingend erforderlich. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen.

§ 3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

(1) Weitergabekontrolle

Bei der elektronischen Übertragung oder dem Transport können personenbezogene Daten nicht gelesen, kopiert, verändert oder entfernt werden und der Empfänger der Daten ist jederzeit bekannt, da folgende Maßnahmen ergriffen werden:

- Datenkommunikation über VPN-Tunnel
- Inhaltsverschlüsselte Datenübertragung
- Überwachung von Fernwartungsaktivitäten
- Fernlöschung von mobilen Endgeräten

(2) Eingabekontrolle

Die Kontrolle der Eingabe, Veränderung und Entfernung bzw. Löschung von personenbezogenen Daten wird durch folgende Maßnahmen umgesetzt:

- Arbeiten mit individuellen Benutzerkennungen
- Protokollierung aller Administratoraktivitäten
- Protokollierung der Datenänderungen
- Protokollierung der Zugriffsversuche
- Berechtigungskonzept mit gesonderten Eingabe-, Änderungs- und Löschbefugnissen
- Datenerfassungsanweisungen
- Plausibilitätskontrollen
- Benutzerkennungsbezogene Protokollierung
- Protokollierung der Dateneingaben
- Protokollierung der Datenlöschungen
- Protokollierung gescheiterter Zugriffsversuche
- Sicherung der Protokolldaten gegen Veränderung und Verlust
- Übersicht der Anwendungen mit Eingabe-, Änderungs- und Löschfunktion

§ 4 Verfügbarkeit und Belastbarkeit

(1) Verfügbarkeitskontrolle

Die verarbeiteten Daten werden durch folgende Maßnahmen gegen zufällige Zerstörung oder Verlust geschützt:

- Sicherungs- und Wiederherstellungskonzept (Backup & Recovery)
- Festgelegte Zuständigkeiten für die Datensicherung
- Notfallplan
- Redundante IT-Systeme
- Unterbrechungsfreie Stromversorgung
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Aufbewahrung der Datensicherung in einem anderen Brandabschnitt
- Regelmäßiger Test der Datenwiederherstellung
- Datenträgerspiegelung (RAID)
- Virtualisierte Infrastruktur
- Überspannungsschutz
- Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen

- Feuerlöscher

(2) Rasche Wiederherstellbarkeit

- Durch Virtualisierung schnelle Disaster-Recovery-Wiederherstellung
- Stündliche Transaktionsprotokolle bei Datenbanken
- Ein Notfallplan und ein Backup-Konzept existieren

§ 5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(1) Datenschutz-Management

Der Auftragnehmer hat einen externen Datenschutzbeauftragten bestellt. Darüber hinaus werden in regelmäßigen Abständen die Datenschutzprozesse und die technisch-organisatorischen Maßnahmen bewertet und optimiert

(2) Auftragskontrolle

Die Sicherstellung der Auftragsdatenverarbeitung nach Weisung des Auftraggebers wird durch folgende Maßnahmen erreicht:

- Dokumentation der getroffenen Sicherheitsmaßnahmen
- Dokumentation und Auskunft über eingesetzte Programme
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Bestellung eines betrieblichen Datenschutzbeauftragten
- Dokumentation und Auskunft über vorhandene IT-Infrastruktur

Ort/Datum

Auftragnehmer
(Zeichnung in Textform: Handelsinhaber, Position)

Anlage 2 Unterauftragsverhältnisse

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer (siehe § 9 (1) „Unterauftragsverhältnisse“) unter der Bedingung des Abschlusses einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu (bitte ankreuzen und ggf. ergänzen)

	Firma Unterauftragnehmer	Anschrift	Leistung
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

.....

(Ort/Datum)

.....

- Auftraggeber –
(Zeichnung in Textform: Handelnder, Position)