Vereinbarung über die Auftragsdatenverarbeitung

Die EDI Center GmbH (im Folgenden „EDICENTER“) sichert dem Auftraggeber gemäß Datenschutzgrundverordnung (DSGVO) die nachfolgenden Maßnahmen im Rahmen der Auftragsdatenverarbeitung zu.

1. Einleitung, Geltungsbereich, Definitionen

(1) Diese Vereinbarung regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In dieser Vereinbarung verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

(4) Die Vereinbarung im Abschnitt „Vertraulichkeit“ gelten über den Bereich der personenbezogenen Daten hinaus, nämlich für sämtliche Tätigkeiten im Bereich von EDI-Dienstleistungen einschließlich deren Anbahnungsphase.

2. Gegenstand und Dauer der Verarbeitung

Das EDICENTER stellt seinem Auftraggeber eine Infrastruktur zur Konvertierung und Übermittlung von EDI-Nachrichten von/an seine Geschäftspartner („EDI-Partner“) sowie damit im Zusammenhang stehende Dienstleistungen, wie z.B. die digitale Signatur für EDI-Rechnungen („eInoice“), zur Verfügung (nachfolgend "Dienstleistung").

Im Rahmen dieser Verarbeitung und zur Erfüllung dieses Vertrags werden personenbezogene Daten erfasst und gespeichert.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsverträgen (im Folgenden „EDI-Vertrag“) einschließlich der zugehörigen Nutzungsbedingungen.

Die Verarbeitung beginnt regelmäßig mit Beginn des EDI-Vertrags und erfolgt auf unbestimmte Zeit bis zur Kündigung dieser Vereinbarung oder des ihr zugrunde liegenden EDI-Vertrags durch eine Partei.

3. Art und Zweck der Datenverarbeitung

Die Verarbeitung ist von folgender Art: Geschäftsbelege werden in elektronischer Form zwischen dem Auftraggeber und dessen EDI-Partner übermittelt und/oder konvertiert. Die personenbezogenen Daten werden zur Kommunikation bei Supportfällen, für Anfragen, Angebote und Abrechnungen verwendet. Eine Weitergabe an Dritte erfolgt nur auf Wunsch des Abonnenten und/oder zum Zweck der Auftragserfüllung.

(z.B. Kommunikation mit dem EDI-Partner des Abonnenten zur Klärung von Störungen). Es erfolgt keine Verarbeitung von personenbezogenen Daten im Sinne von Art. 35, Abs. 3, lit. a,b,c.

4. Art der Daten

Es werden die im EDI-Vertrag vereinbarten Geschäftsbelege in elektronischer Form verarbeitet (z.B. ORDERS, INVOIC, DESADV, usw.). Zusätzlich werden alle für die Kommunikation benötigten Informationen gespeichert (in der Regel Name, Adresse, Firma, Funktion, Telefonnummer, Fax, E-Mail, Web-Adresse).

5. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind alle Ansprechpartner beim Auftraggeber, die für die Kommunikation bei Supportanfragen, Anfragen zur EDI-Vertrags-Erweiterung, Änderung, Kündigung, Abrechnung usw. explizit oder implizit zuständig sind.

6. Pflichten des Auftragnehmers

(1) 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.

(2) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit zu wahren.

(3) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden.

(5) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten.

(6) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(7) Auskünfte an Dritte darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(8) Der Auftragnehmer bestellt eine fachkundige und zuverlässige Person als Datenschutzbeauftragten. In Zweifelsfällen kann sich der Auftraggeber direkt an diesen wenden. Die Kontaktdaten des Datenschutzbeauftragten werden auf der Homepage des Auftragnehmers veröffentlicht.

(9) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter Einhaltung der Bestimmungen dieses Vertrags erfolgen.

7. Technische und organisatorische Maßnahmen

(1) Die im Anhang beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen.

(6) Die Verarbeitung von Daten in Privatwohnungen sowie die Verarbeitung von Daten im Auftrag mit Privatgeräten ist nicht gestattet.

(7) Dedizierte Datenträger, die vom Auftraggeber stammen, sind angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein.

8. Berichtigung, Löschung und Sperrung von Daten

Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer innerhalb von dreißig Tagen nach Bekanntwerden der Anforderung berichtigen, löschen oder sperren. Dies gilt auch über die Beendigung dieses Vertrages hinaus.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist zulässig, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind.

(2) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(3) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(4) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich im Gebiet der EU oder des EWR erbringen, ist nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(5) Zurzeit sind keine Subunternehmer mit der Verarbeitung von personenbezogenen Daten beauftragt. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen.

(6) Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung, die Inanspruchnahme von Telekommunikationsdienstleistungen einschließlich E-Mal sowie kaufmännische und steuerliche Dienstleistungen werden nicht aufgelistet. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

10. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken. Das Betriebsgeheimnis ist in jedem Fall zu wahren.

11. Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber relevante Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 72 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d. eine Beschreibung der vom Auftragnehmer vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

12. Weisungen

(1) Der Auftraggeber benennt die zur Erteilung und Annahme von Weisungen ausschließlich befugte Person. Beim Auftragnehmer ist der Datenschutzbeauftragte die beauftragte Person.

(2) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(3) 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 solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(4) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

13. Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

14. Vertraulichkeit

Die Parteien garantieren sich gegenseitig Vertraulichkeit. Dies gilt für sämtliche Tätigkeiten im Bereich von EDI-Dienstleistungen einschließlich deren Anbahnungsphase. Vertrauliche Informationen im Sinne dieser Vereinbarung sind:

a. Sämtliche personenbezogenen Daten
b. Alle mündlichen oder schriftlichen Informationen und Materialien, die der Auftragnehmer direkt oder indirekt vom Auftragnehmer zur Abwicklung des Auftrages erhält und als vertraulich gekennzeichnet sind oder deren Vertraulichkeit sich aus ihrem Gegenstand oder sonstigen Umständen ergibt.
c. Alle Geschäftsdaten des Auftraggebers, insbesondere die Inhalte der vom EDICENTER zu verarbeitenden EDI-Dateien.
d. Die beauftragten Leistungen und sonstige Arbeitsergebnisse.

Jede Partei verpflichten sich, alle ihr direkt oder indirekt zur Kenntnis gekommenen vertraulichen Informationen als solche zu behandeln und nicht ohne Zustimmung der jeweils anderen Partei an Dritte weiterzugeben, zu verwerten oder zu verwenden.

Die Verpflichtung zur Vertraulichkeit gilt nicht, wenn eine Pflicht zur Offenlegung der vertraulichen Information durch Beschluss eines Gerichts, Anordnung einer Behörde oder ein Gesetz besteht.

Die Parteien werden alle geeigneten Vorkehrungen treffen, um die Vertraulichkeit sicherzustellen. Vertrauliche Informationen werden nur an die Mitarbeiter oder sonstige Dritte weitergegeben, die sie aufgrund ihrer Tätigkeit erhalten müssen. Die Parteien stellen sicher, dass die zum Einsatz kommenden Personen die vorliegende Vertraulichkeitsvereinbarung ebenfalls beachten.

Die Pflicht zur Vertraulichkeit dauert auch nach Beendigung der Zusammenarbeit an. Auf Verlangen sind ausgehändigte Unterlagen einschließlich aller davon angefertigten Kopien sowie Arbeitsunterlagen und -Materialien zurückzugeben.

15. Vergütung

Die Vergütung des Auftragnehmers ist abschließend im EDI-Vertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

16. Haftung

Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen. Dies gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist. Die Haftungssumme ist auf sechs Monatsgebühren des betroffenen EDI-Vertrags begrenzt.

17. Sonderkündigungsrecht

(1) Der Auftraggeber kann den EDI-Vertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

Der Auftragnehmer hat dem Auftraggeber alle direkten Kosten zu erstatten, die diesem durch die verfrühte Beendigung des EDI-Vertrags oder dieses Vertrages in Folge einer berechtigten außerordentlichen Kündigung

durch den Aufraggeber entstehen. Die Erstattungssumme ist auf sechs Monatsgebühren des betroffenen EDI-Vertrags begrenzt. Entgangener Gewinn bleibt von der Erstattung ausgeschlossen.

18. Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

19. Schlussbestimmungen

(1) Diese Vereinbarung gilt auch für die Rechtsnachfolger der Parteien. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

(2) Diese Vereinbarung unterliegt dem Deutschen Recht. Gerichtsstand ist Augsburg.

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

Neusäß, den 16.05.2018

Ihr EDICENTER

-> Anlage „Technische und organisatorische Maßnahmen“

Anlage „Technische und organisatorische Maßnahmen“

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

1. Gewährleistung der Vertraulichkeit

Zutrittskontrolle: *(Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.)*	☒ Alarmanlage ☒ manuelles Schließsystem ☒ Schließsystem mit Sicherheitsschlössern ☒ Bewegungsmelder ☒ Schlüsselregelung Beschäftigte ☒ Verschließen der Türen bei Abwesenheit
Zugangskontrolle: *(Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)*	☒ Erstellen von Benutzerprofilen mit unterschiedlichen Berechtigungen ☒ Pflicht zur Passwortnutzung ☒ Authentifikation durch Benutzername und Passwort ☒ Einsatz von sicherer Technologie bei Zugriff von außen auf die internen Systeme
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*	☒ Nutzer-Berechtigungskonzept ☒ Verwaltung der Nutzerrechte durch Systemadministrator ☒ Anzahl der Administratoren auf das Notwendigste reduziert

der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.)	☒ Einsatz von Aktenvernichtern oder von Dienstleistern zur Aktenvernichtung (inkl. Protokollierung der Vernichtung) ☒ Aufbewahrung von Datenträgern in abschließbaren Schränken/Tresor ☒ Aufbewahrung von Aktenordnern in abschließbaren Schränken ☒ ordnungsgemäße Vernichtung von Datenträgern
Trennungsgebot: *(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.)*	☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern ☒ logische Mandantentrennung ☒ Festlegung von Datenbankrechten durch Vorgaben im Berechtigungskonzept
Auftragskontrolle: *(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.)*	☒ schriftliche Vereinbarung mit dem Auftragnehmer ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit ☒ Datenschutzbeauftragter beim Auftragnehmer ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

2. Gewährleistung der Integrität

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 im System ☒ individuelle Benutzernamen für Nutzer ☒ sichere Aufbewahrung von Papierunterlagen, von denen Daten ins EDV-System übernommen wurden

	☒ Nachvollziehbarkeit durch Berechtigungskonzept
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.)*	☒ verschlüsselte Datenübertragung ☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form (wenn möglich) ☐ verschlüsselte E-Mail-Übertragung (SSL/TLS) ☐ Verschlüsselung E-Mail-Inhalte (Software-Zertifikat) ☒ festgelegte Löschfristen

3. Gewährleistung der Verfügbarkeit

Verfügbarkeitskontrolle: *(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)*	☒ unterbrechungsfreie Stromversorgung (USV) für Server ☒ Alarmanlage ☒ Klimaanlage in Serverräumen ☒ Überwachung von Temperatur und Feuchtigkeit in Serverräumen ☒ Schutzsteckdosenleisten für EDV-Geräte ☒ Feuer- bzw. Rauchmeldeanlagen ☒ Feuerlöschgeräte ☒ Datensicherungs-Konzept ☒ regelmäßiges Testen der Funktionsweise der Datensicherung ☒ Notfallkonzept (Handbuch) ☒ Aufbewahrung von Datensicherung an sicherem, ausgelagertem Ort

	☒ Serverräume nicht unterhalb von sanitären Anlagen gelegen ☒ keine Wasserleitungen über Server-Rechnern ☒ Serverräume nicht in Hochwasser gefährdeten Kellerräumen ☒ zusätzlicher Hochwasserschutz: Server auf Sockeln

4. Gewährleistung der Belastbarkeit der Systeme

Belastbarkeit der IT-Systeme:	☒ Antiviren-Software ☒ Hardware-Firewall ☒ Software-Firewall ☒ sorgfältige Auswahl des externen IT-Dienstleisters

5. Wiederherstellung der Verfügbarkeit

Wiederherstellbarkeit von IT-Systemen:	☒ sorgfältig ausgewählter interner System-Administrator ☒ Vorhaltung von Ersatz-Hardware / Server ☒ Ausgefeiltes Wiederherstellungskonzept für verschiedene Ausfallszenarien