Vertrag über die Auftragsverarbeitung personenbezogener Daten Wartung und Pflege des EBIS-Programmes sowie Durchführung der jährlichen Auswertung gemäß Art. 28 Datenschutzgrundverordnung (DS-GVO) und § 30 Gesetz über den kirchlichen Datenschutz (KDG) und § 30 des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG-EKD)

zwischen

vertreten durch

im Folgenden: **Auftraggeber**

und

GSDA GmbH
Kapellenstraße 13
85622 Feldkirchen b. München

vertreten durch

Karlheinz Pelzel
Michael Strobl

im Folgenden: **Auftragnehmer**

1 Einleitung, Geltungsbereich, Definitionen

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

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

(3) In diesem Vertrag 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. Auftragnehmer und Auftraggeber schließen hiermit einen Vertrag gemäß Art. 28 Datenschutzgrundverordnung (DS-GVO) und § 30 Gesetz über den kirchlichen Datenschutz (KDG) und § 30 des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG-EKD) ab. Zum Zweck der einfachen Lesbarkeit wird im Folgenden nur auf die DS-GVO referenziert.

2 Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Teilnahmeerklärung EBIS und des mit uns abgeschlossenen Fernwartungsvertrages (Anhang I, AGB).

2.2 Dauer

Die Verarbeitung beginnt mit der Unterschrift der Teilnahmeerklärung und auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

3 Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

3.1 Art und Zweck der Verarbeitung

Die von Auftragnehmer ausgeführte Datenverarbeitung erfolgt standardmäßig zum Zweck der Vertragsdurchführung und der Auswertung und Wartung sowie in Einzelfällen die Datenprüfung und ggf. -korrektur bei technischen Problemen.

Sollten die Korrekturen nicht auf den originalen Datenablagesystemen möglich sein, können die Daten zu diesem Zweck auch an die GSDA übermittelt und dort bearbeitet werden. Als zulässiger Übermittlungsweg für diese Fälle ist die Dateiübertragung per TeamViewer® oder per verschlüsselte Zip-Datei.

3.2 Art der Daten

Die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer beschränkt sich auf den Kreis der

- Einrichtungsdaten (Adresse der Einrichtung)
- Ansprechpartner in der Einrichtung
- Telefon- und Email-Kontakt der Einrichtung
- Zahlungsinformationen der Einrichtung
- Klientendaten, dazu gehören Stammdaten, Kontaktdaten, allgemeine Angaben zur Familie, Fallakten und etwaiger Schriftverkehr.

3.3 Kategorien betroffener Personen

Der Kreis der von dieser Verarbeitung Betroffenen umfasst die Einrichtung selber sowie die Verarbeitung bei der Wartung des EBIS-Systems die Klienten des Auftraggebers sowie etwaige Bezugspersonen der Klienten.

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

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

(3) Die eingesetzten Mitarbeiter sind auf das Datengeheimnis verpflichtet. Mitarbeitende, die auf besondere Kategorien personenbezogener Daten zugreifen können, sind nach § 203 Strafgesetzbuch verpflichtet.

(4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen gemäß der jeweils geltenden gesetzlichen Bestimmungen vor Beginn der Verarbeitung vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(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 und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

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

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

(8) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten unter datenschutz@gsda.de wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(9) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

(10) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche

Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

(11) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 Abs. 1 und 2 DSGVO sowie § 31 KDG. Er stellt dem Auftraggeber auf Anforderung die für die Übersicht nach § 31 KDG notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

5 Technische und organisatorische Maßnahmen

(1) Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(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.. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren. Die aktuelle Liste unserer technisch-organisatorischen Maßnahmen (Anlage 1) finden Sie unter https://www.gsda.de/dsgvo.html.

(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 strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Die Verarbeitung von Daten in Privatwohnungen ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

(7) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(8) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis wird dem Auftraggeber jederzeit auf Anforderung überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

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

(5) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

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

(7) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

(8) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere 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.

(9) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

(10) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(11) Die aktuelle Liste (Anlage 2) unserer eingesetzten Subunternehmer finden Sie unter https://www.gsda.de/dsgvo.html

(12) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind

nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 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 und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(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 wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 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 ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(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.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 3.

(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.

11 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. Eine physische Vernichtung erfolgt gemäß DIN 66399.

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

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(4) 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.

12 Vergütung

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

13 Haftung

(1) Hier gelten die Bestimmungen des Art. 82 DSGVO.

14 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. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als 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.

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

_____	_____
Unterschriften: Auftraggeber	Karl-Heinz Pelzel
	Geschäftsführer GSDA GmbH
	Auftragnehmer

Die aktuelle Liste unserer technisch-organisatorischen Maßnahmen (Anlage 1) finden Sie unter https://www.gsda.de/dsgvo.html

Anlage 1 – technische und organisatorische Maßnahmen

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit. 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.

Vertraulichkeit

1. Zutrittskontrolle

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

- ☒ Alarmanlage
- ☒ Sicherheitsschlösser
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Sorgfältige Auswahl von Wachpersonal

2. Zugangskontrolle

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

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☒ Sorgfältige Auswahl von Wachpersonal
- ☒ Verschlüsselung von mobilen Datenträgern
- ☒ Erstellen von Benutzerprofilen
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☒ Sicherheitsschlösser
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Verschlüsselung von Datenträgern in Laptops / Notebooks
- ☒ Einsatz einer Software-Firewall

☒ Einsatz von Anti-Viren-Software

2. 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

☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☒ physische Löschung von Datenträgern vor Wiederverwendung

☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☒ Verwaltung der Rechte durch Systemadministrator

☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☒ Sichere Aufbewahrung von Datenträgern

☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☒ Protokollierung der Vernichtung

3. 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

☒ Festlegung von Datenbankrechten

☒ Logische Mandantentrennung (softwareseitig)

☒ Trennung von Produktiv- und Testsystem

Integrität

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, 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 (auf Kundenwunsch)

☒ E-Mail-Verschlüsselung

☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Feuerlöschgeräte vor Serverräumen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Testen von Datenwiederherstellung
- ☒ Erstellen eines Notfallplans
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Serverräume nicht unter sanitären Anlagen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. 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)
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis nach DSGV
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ Vertragsstrafen bei Verstößen

Die aktuelle Liste unserer eingesetzten Subunternehmer finden Sie unter https://www.gsda.de/dsgvo.html

Unterauftragnehmer	**Anschrift/Land**	**Leistung**
Kloppe Media	Ansbacher Str. 85 D - 91541 Rothenburg	SMS-Gateway-Betreiber (wird nur benötigt, wenn die SMS-Funktion in EBIS eingesetzt wird)
Susanne Novi	Waldweg 5 84094 Elsendorf	Hotline-Unterstützung

Anlage 3 – Weisungsberechtige Personen

Folgende Personen sind zur Entgegennahme von Weisungen beim Auftragnehmer befugt:

Name:	Herr Karlheinz Pelzel
Position:	Geschäftsführer
Tel.	089 997406963
E-Mail	pelzel@gsda.de

Folgende Personen sind beim Auftraggeber zur Erteilung von Weisungen befugt:

Name: _____

Position: _____

Tel. _____

E-Mail _____

-