Auftragsverarbeitungsvereinbarung

Zwischen

Name der verantwortlichen Stelle
Straße, Hausnummer
Postleitzahl, Ort

- Auftraggeber -

und

BSG Brandschutz-Sicherheit-Grafik GmbH
Sachverständigenbüro für Brandschutz
Breitscheidstraße 84
01237 Dresden

- Auftragnehmer -

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz nach Art. 28 Abs. 3 DS-GVO, die sich aus der in der Leistungsvereinbarung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet auf alle Tätigkeiten Anwendung, die mit der Leistungsvereinbarung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten des Auftraggebers verarbeiten.

§ 1 Gegenstand, Ort und Dauer der Vereinbarung

(1) Der Auftragnehmer erbringt für den Auftraggeber die in der Leistungsvereinbarung beschriebenen Leistungen.

(2) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der europäischen Kommission, EU-Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(3) Die Dauer dieser Vereinbarung entspricht der Laufzeit der Leistungsvereinbarung.

Darüber hinaus ist eine vorzeitige Beendigung dieses Auftrages, ohne Einhaltung einer Kündigungsfrist im Falle einer schwerwiegenden Verletzung von gesetzlichen und/oder vertraglichen Datenschutzbestimmungen zulässig, sofern das Festhalten an dieser Vereinbarung für die jeweilige Vertragspartei unzumutbar ist. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

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.

§ 2 Art und Zweck der Verarbeitung, Kategorie betroffener Personen, Art der Daten

(1) Die Art, der Umfang und der Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten richtet sich nach dem zwischen den Parteien konkret vereinbarten Hauptvertrag in der aktuell gültigen Fassung (und der dazugehörigen Leistungsbeschreibung).

(2) Art der personenbezogenen Daten (vgl. Art. 4 Nr. 1, sowie ggf. Nr. 13 bis 15 DS-GVO):

☐ Personenstammdaten (z.B. Name, Vorname, Anschrift, Geburtsdatum)

☐ Kommunikationsdaten (z.B. Telefon, E-Mail)

☐ Vertragsstammdaten (z.B. Vertragsbeziehungen, Produkt- und Vertragsinteresse)

☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten (z.B. Lohn, Gehalt, Reisekosten)

☐ Planungs- und Steuerungsdaten

☐ IT-Nutzungsdaten (z.B. UserID, Passwörter, Rollen)

☐ Bankdaten (z.B. Kontoverbindungen und Kreditkartennummern)

☐ Bonitätsdaten (z.B. Zahlungsverhalten und Bilanzen)

☐ Sonstige: ***

(zutreffendes bitte ankreuzen/ergänzen)

(3) Kategorien betroffener Personen (vgl. Art. 4 Nr. 1 DS-GVO):

☐ Beschäftigte

☐ Kunden

☐ Interessenten

☐ Lieferanten / Dienstleister

☐ Handelsvertreter / Berater

☐ Ansprechpartner

☐ Geschäftspartner

☐ Sonstige: ***

(zutreffendes bitte ankreuzen/ergänzen)

§ 3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO ist allein für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der auftragsgemäßen Verarbeitung verantwortlich. Die alleinige Verantwortlichkeit des Auftraggebers erstreckt sich auch auf die Wahrung der Betroffenenrechte nach Art. 12 bis Art. 22 DS-GVO. Der Auftragnehmer verarbeitet die Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers.

Die Weisungen werden anfänglich durch den Vertrag festgelegt. Der Auftraggeber ist berechtigt, im Rahmen des Auftrags Einzelweisungen zu erteilen. Er erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. In begründeten Einzelfällen können durch Bevollmächtigte des Auftraggebers Weisungen auch mündlich erteilt werden. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre zu Nachweiszwecken aufzubewahren.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO) Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

(2) Die Vertragsparteien vereinbaren als Weisungsberechtigte und für die Annahme von Weisungen folgende Ansprechpartner:

Weisungsberechtigte Personen des Auftraggebers sind:

Vor- und Nachname: ***
Telefonnummer: ***
E-Mail: ***

Vor- und Nachname: ***
Telefonnummer: ***
E-Mail: ***

Weisungsempfänger beim Auftragnehmer sind:

Vor- und Nachname: Jens Breutmann
Telefonnummer: 0651 4113379
E-Mail: jens.breutmann@bsg-online.de

Vor- und Nachname: Annett Oehmigen
Telefonnummer: 034491 22507
E-Mail: annett.oehmigen@bsg-online.de

Bei einem Wechsel oder einer Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich schriftlich oder in einem dokumentierten elektronischen Format die Nachfolger bzw. Vertreter mitzuteilen.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Eine darüberhinausgehende Verarbeitung ist nur in dem Umfang zulässig, in dem der Auftragnehmer zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist (z.B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der

Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet (vgl. Art. 28 Abs. 3 Satz 2 a DS-GVO).

(2) Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, Sicherheitskopien (soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind) sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(3) Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen scharf getrennt werden.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) ☒ Der Auftragnehmer hat folgende Person als Beauftragte für den Datenschutz benannt:

DID DRESDNER INSTITUT FÜR DATENSCHUTZ
Telefonnummer: +49 351 655 772 - 0
E-Mail: zentrale@dids.de

Ein Wechsel des Datenschutzbeauftragten oder eine Änderung der innerbetrieblichen Aufgaben desselben sind dem Auftraggeber unverzüglich unter Nennung der Kontaktdaten mitzuteilen.

☐ Der Auftragnehmer ist gemäß den einschlägigen datenschutzrechtlichen Vorschriften nicht zur Benennung eines Datenschutzbeauftragten verpflichtet.

(6) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Die derzeit beim Auftragnehmer getroffenen Maßnahmen sind in Anlage 1 aufgeführt. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) mitteilen.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Wenn und soweit die dazu erforderlichen Maßnahmen über den in der Leistungsbeschreibung des Vertrages enthaltenen Umfang hinausgehen, vergütet der Auftraggeber diese gesondert.

(9) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Der Auftraggeber trägt die Kosten der Unterstützung.

§ 5 Kontrollrechte und -pflichten

(1) Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften, Nachweisen und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort in dem Geschäftsbetrieb des Auftragnehmers (Art. 28 Abs. 3 Satz 2 h DS-GVO). 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.

(4) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

§ 6 Mitwirkungspflichten des Auftragnehmers

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

(2) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis Art. 36 DS-GVO genannten Pflichten.

(3) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht aus Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt insbesondere auch in Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33, Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33, Art. 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. f) DS-GVO). Meldungen für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

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

(5) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

§ 7 Unterauftragsverhältnisse mit Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 2 genannten Subunternehmer durchgeführt. Mit deren Beauftragung erklärt sich der Auftraggeber im dargestellten Umfang einverstanden.

(2) Andere Unterauftragsverarbeiter darf der Auftragnehmer nur einsetzen, hinzuziehen oder bestehende ersetzen, wenn er die Auftraggeber zuvor über die beabsichtigte Änderung informiert hat und die Auftraggeber gegen derartige Veränderung nicht binnen 10 Tagen Einspruch erhoben haben. Der Einspruch darf nicht ohne wichtigen datenschutzrechtlichen Grund erhoben werden und bedarf einer angemessenen Begründung der Auftraggeber (schriftlich oder in einem dokumentierten elektronischen Format) aus datenschutzrechtlicher Sicht.

(3) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung in eigener Verantwortung beauftragt. 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 und die Entsorgung von Datenträgern des Auftragnehmers sind nicht erfasst.

(4) Eine Beauftragung von Subunternehmen in Drittstaaten darf darüber hinaus nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 DS-GVO erfüllt sind (z.B. Angemessenheitsbeschluss der europäischen Kommission, EU-Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(5) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und 9 DS-GVO). In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden.

§ 8 Löschung

(1) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung der Löschung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(2) Ist eine datenschutzkonforme Löschung durch den Auftragnehmer nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien oder händigt die entsprechenden Datenträger dem Auftraggeber aus.

§ 9 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) Ergänzungen und Änderungen dieser Vereinbarung bedürfen der Schriftform.

(3) Soweit Erklärungen, Informationen und Dokumentationen „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) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(5) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(6) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist Schmölln oder Dresden, Deutschland.

Schmölln, den 01.12.2024

_____, den _____

Jens Breutmann
Auftragnehmer

_____
Auftraggeber

Anlage 1: Technische und organisatorische Maßnahmen (TOM)

Vertraulichkeit

Zutrittskontrolle: *Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verweigert.*

☐ Sicherheitsschlösser	☐ Personenkontrolle durch Empfang
☒ Manuelles Schließsystem	☐ Protokollierung der Besucher
☐ Chipkarten-/Transponder-Schließsystem	☒ Begleitung von Besuchern
☐ Biometrische Zugangssperren	☐ Tragepflicht von Berechtigungsausweisen
☐ Automatisches Zutrittskontrollsystem	☐ Sorgfältige Auswahl von Wachpersonal
☒ Schlüsselregelung	☐ Sorgfältige Auswahl von Reinigungspersonal
☐ Alarmanlage	☐ Absicherung von Gebäudeschächten
☒ Klingelanlage mit Kamera	☐
☐ Lichtschranke / Bewegungsmelde	☐
☐ Videoüberwachung der Zugänge	☐

Zugangskontrolle: *Unbefugten wird die Nutzung von Datenverarbeitungssystemen verhindert.*

☒ Vergabe von Benutzerrechten	☒ Zentrale Administrationssoftware
☒ Passwortrichtlinie	☒ Software-Firewall
☐ Zentrale Passwortvergabe	☒ Hardware-Firewall
☒ Authentifikation mit Benutzername und Passwort	☐ Intrusion-Detection-Systeme
☒ Authentifikation mit biometrischen Verfahren	☐ Verwendung von VPN-Verbindungen
☐ Verhinderung lokaler Speicherung v. Passwörtern	☐ Antiviren-Software Client
☒ Automatische Sperrung v. Geräten bei Inaktivität	☒ Antiviren-Software Server
☒ Sperrung von Schnittstellen (z.B. USB-Schnittst.)	☐
☒ Beschränkung auf firmeneigene Datenträger	☐
☐ Patchmanagement für OS und Anwendungen	☐

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

☒ Abgestufte Vergabe von Benutzerrechten	☐ Löschung v. Datenträgern vor Wiederverwendung
☒ Protokollierung von Zugriffen	☐ Ordnungsgemäße Vernichtung von Datenträgern
☒ Rechteverwaltung durch Systemadministrator	☐ Einsatz geeigneter Aktenvernichter / Dienstleister
☒ Minimale Anzahl an Administratoren	☐ Sichere Aufbewahrung von Datenträgern
☐ Gesonderter Passwortschutz für Anwendungen	☐
☐ Automatische Sperrmechanismen	☐

☐ Verschlüsselung von mobilen Datenträgern	☐

Trennungskontrolle: *Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

☐ Physische Trennung	☐ Sandboxing / Trennung v. Produktiv- & Testsystem
☐ Softwareseitige Trennung	☐
☐ Verwendung von Zweckattributen / Datenfeldern	☐
☐ Berechtigungskonzept	☐

Pseudonymisierung: *Gewährleistung der Verarbeitung personenbezogener Daten in einer Weise, in der 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.*

☐ Nutzung von Pseudonymen	☐
☐ Geeignete Wahl der Pseudonymisierungsschlüssel	☐
☐ Getrennte Aufbewahrung der Zuordnungsdatei	☐

Integrität

Weitergabekontrolle: *Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

☐ Keine unbefugte Entnahme von Daten möglich	☐ Übersicht der Abruf- und Übermittlungsvorgänge
☐ Dokumentation eventueller Datenentnahmen	☐ Sorgfältige Auswahl der Übermittlungswege
☐ E-Mail-Verschlüsselung	☐ Sorgfältige Auswahl von Transportbehältern
☐ Verwendung elektronischer Signaturen	☐ Nutzung verschlüsselter Verbindungen (z.B. https)
☐ Weitergabe in ano-/pseudonymisierter Form	☐
☐ Dokumentation von Empfängern	☐

Eingabekontrolle: *Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

☐ Dokumentenmanagement	☐ Festgelegte Zuständigkeiten für Löschungen
☐ Protokollierung von Änderungen an Daten	☐
☐ Überprüfung von Protokolldateien	☐

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: *Gewährleistung, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*

☐ Gespiegelte Festplatten, Systeme / Cluster	☐ Regelmäßige Datenwiederherstellungstests
☐ Unterbrechungsfreie Stromversorgung	☐ Sichere Aufbewahrung von Datensicherungen
☐ Überspannungsschutz	☐ Wartungsverträge mit geeigneter Reaktionszeit
☐ Software-Firewall	☐ Feuer- und Rauchmeldeanlagen
☐ Hardware-Firewall	☐
☐ Aktualisierung / Härtung der Systeme	☐
☐ Backup- und Recoverykonzept	☐

Rasche Wiederherstellbarkeit: *Gewährleistung, dass personenbezogene Daten im Falle von Zerstörung oder Verlust zeitnah wiederhergestellt werden können.*

☐ Notfallplan (z.B. BSI IT-Grundschutz 100-4)	☐ Eigene Ersatzteilbevorratung
☐ Regelung von Zuständigkeiten und Abläufen	☐
☐ Nutzung virtueller Systeme mit Off-site-Sicherung	☐
☐ Hardware-Service-Verträge	☐

Verfahren zur regelmäßigen Überprüfung & Evaluierung

Datenschutz-Management: *Maßnahmen und Prozesse zur Etablierung eines DS-GVO-gerechten Datenschutzniveaus.*

☐ Bestellung eines Datenschutzbeauftragten	☐ Prozess zur Reaktion auf Datenschutzverletzungen
☐ Einsatz von Datenschutzkoordinatoren	☐ Arbeitsanweisungen mit Datenschutzhintergrund
☐ Aktuelles Verzeichnis der Verarbeitungstätigkeiten	☐ Sicherheitszertifizierungen (z.B. ISO 27001)
☐ Durchführung v. Datenschutz-Folgeabschätzungen	☐ Informationssicherheitskonzept vorhanden
☐ Sensibilisierung der Beschäftigten	☐ Review Prozesse
☐ Verpflichtung d. Beschäftigten auf Vertraulichkeit	☐
☐ Erfüllung von Informationspflichten	☐
☐ Prozess zur Bearbeitung von Betroffenenanfragen	☐

Incident-Response-Management: *Definition der Organisation zum Umgang mit Datenschutzvorfällen.*

☐ Einsatz / regelmäßige Aktualisierung v. Firewalls	☐ Prüfung / Risikoklassifizierung von Vorfällen
☐ Einsatz / regelmäßige Aktualisierung v. Spamfiltern	☐ Vorbereitete Reaktionen auf Vorfälle
☐ Definition von Zuständigkeiten bei Vorfällen	☐ Reflexion und Nachbereitungsprozesse
☐ Einbindung des Datenschutzbeauftragten	☐
☐ Definierte Meldeprozesse und Eskalationswege	☐
☐ Aktuelle Melde- und Kontaktlisten	☐

Datenschutzfreundliche Technikgestaltung und Voreinstellung: *Maßnahmen gemäß Art. 25 DS-GVO.*

☐ Sicherstellung von Privacy by Design	☐

☐ Sicherstellung von Privacy by Default	☐

Auftragskontrolle: *Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können sowie Maßnahmen bei Outsourcing von Datenverarbeitungen an Auftragsverarbeiter.*

☐ Auftragsverarbeitungsverträge	☐ Verpflichtung der Vertraulichkeit
☐ Festgelegte Verpflichtungen & Zuständigkeiten	☐ Vereinbarung von Kontrollrechten
☐ Verschriftlichung von Weisungen	☐ Laufende Überprüfung von Auftragsverarbeitern
☐ Vernichtung von Daten nach Vertragsbeendigung	☐
☐ Sorgfältige Auswahl von Auftragsverarbeitern	☐
☐ Prüfung der TOM von Auftragsverarbeitern	☐

Anlage 2: Subunternehmen (weitere Auftragsverarbeiter)

Name und Anschrift des Subunternehmens	Gegenstand der Unterbeauftragung	Geeignete Garantien gemäß Art. 46 DS-GVO bei Subunternehmen in Drittstaaten