Vereinbarung zur Verarbeitung von Daten im Auftrag nach Art. 28 DSGVO

zwischen

BMS Büro & Marketing – Service e.K., Königstraße 80 in 70173 Stuttgart (Auftragsverarbeiter - nachstehend **Auftragnehmer** genannt) und dem

Kunden (Verantwortlicher - nachstehend **Auftraggeber** genannt) (gemeinsam nachfolgend „**die Parteien**")

1. Gegenstand und Dauer des Auftrags

Der Auftragnehmer führt im Auftrag des Auftraggebers für die Dauer der Vertragslaufzeit eine Verarbeitung personenbezogener Daten auf Grundlage des Hauptvertrages aus.
Der Gegenstand der Verarbeitung ist im Hauptvertrag und in Anlage 1 Leistungsvereinbarung zu diesem AVV festgelegt.
Der sich aus dem Hauptvertrag ergebende Leistungsumfang kann – je nach gebuchter Leistung – eine oder mehrere der in Anlage 1 Leistungsvereinbarung genannten Verarbeitungsvorgänge beinhalten – ohne dass hierdurch die Leistungspflichten neu definiert werden.

Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung. Es gelten die Kündigungsfristen des Vertrages über Bürodienstleistungen.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten/Art der Daten/Kategorien betroffener Personen

Die Art und der Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1 Leistungsvereinbarung.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen. Einzelheiten siehe Anlage 2 TOM.

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

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Der Auftraggeber erteilt dem Auftragnehmer – abweichend von (1) dieses Absatzes 4 - die Genehmigung, soweit zutreffend und es Telefondienstleistungen betrifft, die vom Auftragnehmer aufgenommenen Anruferdaten zu speichern und im Rahmen der Leistungsvereinbarung zu ändern oder zu bearbeiten, soweit es notwendig ist, um die gewünschten Dienstleistungen ordnungsgemäß zu erbringen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer verpflichtet sich einen Datenschutzbeauftragten oder, falls er dazu gesetzlich nicht verpflichtet ist, einen sonstigen Ansprechpartner zu ernennen, der für Fragen des Datenschutzes verantwortlich zeichnet. Der Auftragnehmer trägt Sorge dafür, dass die Person über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen verantwortlichen Person können der Anlage 3 Datenschutzbeauftragter entnommen werden.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO. Einzelheiten siehe Anlage 2 TOM.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO 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 Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(6) Die vom Auftragnehmer beauftragten Unterauftragnehmer sind in Anlage 4 Unterauftragnehmer aufgeführt.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(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 Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- ☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Der Vergütungsanspruch ist bei Anmeldung von Kontrollen mit dem Auftraggeber zu vereinbaren.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO 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 Verletzungsereignissen 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-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen nach Abschnitt 8 (1) d) und e) sowie Unterstützungsleistungen die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber auf Anforderung unverzüglich (mind. 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftraggeber hat dem Auftragnehmer bei einem Wechsel oder einer langfristigen Verhinderung des Auftraggebers unverzüglich einen Nachfolger oder einen Vertreter als Weisungsbefugten mitzuteilen.

10. 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 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) 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.

(4) Personenbezogene Daten der betroffenen Personen werden nur so lange gespeichert, wie dies zur Erfüllung des Zwecks des jeweiligen Datenverarbeitungsvorgangs erforderlich ist und soweit der Löschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen.

11. Haftung

Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers oder etwaiger Unterauftragnehmer gegen diesen Vertrag sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen gelten die Haftungsregelungen aus dem Vertrag über Bürodienstleistungen (AGB).

12. Sonstiges

(1) Sollten die Daten des Auftraggebers bzw. dessen Kunden beim Auftragnehmer oder Subunternehmer 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 an den Daten beim Auftraggeber liegt.

(2) Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die ganz oder teilweise unwirksame Regelung soll durch eine Regelung ersetzt werden, die dem Sinn und Zweck der Unwirksamkeit möglichst nahekommt und die die Parteien vereinbart hätten, wenn sie die Unwirksamkeit gekannt hätten. Entsprechendes gilt, wenn in dieser Vereinbarung eine Lücke offenbart werden sollte.

(4) Es gilt deutsches Recht.

(5) Der Gerichtsstand ist Stuttgart.

Anlagen:

Anlage 1: Leistungsvereinbarung

Anlage 2: Technisch- organisatorische Maßnahmen

Anlage 3: Datenschutzbeauftragter

Anlage 4: Unterauftragnehmer

Anlage 1 - Leistungsvereinbarung

1. Gegenstand und Dauer des Auftrags

- Das Öffnen der Eingangspost, das Scannen der Inhalte und das Weiterleiten per E-Mail, Fax oder ähnlich.
- Das Weiterleiten eingehender Faxe per E-Mail, Fax oder ähnlich.
- Das Erbringen von Büroservicetätigkeiten, wie Schreibarbeiten und Auftragsbearbeitung.
- Die Erfassung und Speicherung von Daten persönlich erscheinender Personen und die Übermittlung per E-Mail oder ähnlich oder durch Übergabe von Ausdrucken.
- Telefonservice in Form der Annahme von Telefonaten in Namen des Auftraggebers, dem Vermitteln von Gesprächen zu vereinbarten Zielen sowie die Erfassung und Speicherung von Anruferdaten und die Übermittlung (per E-Mail, Fax, SMS, durch Übergabe von Ausdrucken oder Eingabe/Speichern in der vom Auftraggeber verwaltete und zur Verfügung gestellte Onlineplattform).

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Art der Verarbeitung von personenbezogenen Daten ergibt sich aus dem gebuchten Leistungsumfang gemäß Hauptvertrag – siehe auch unter Punkt 1: Gegenstand und Dauer des Auftrags.

Der Zweck der Verarbeitung von personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber ist das Ausgliedern von Büro- und Telefonserviceleistungen zur Unterstützung bei der Erledigung von Geschäftsprozessen des Auftraggebers.

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. Jede Verlagerung 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. Das angemessene Schutzniveau in Deutschland ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

(2) Art der Daten

- Personenstamm- und Kontaktdaten (u.a. Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum etc.)
- Telefonate (Gesprächsinhalte, Datum, Uhrzeit
- Eingehende Faxe
- Eingehende Post aller Art
- Vertrags-, Abrechnungs- und Buchungsdaten
- Weitere, nicht absehbare Daten

(3) Kategorien betroffener Personen

- Mitarbeiter/Rentner des Auftraggebers
- Kunden des Auftraggebers
- Interessenten des Auftraggebers
- Anrufer des Auftraggebers
- Sonstige, nicht absehbare Kategorien von Betroffenen

Anlage 2 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle:

- ☐ Alarmanlage
- ☐ Automatisches Zugangskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☐ Lichtschranken/Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☒ Während der Öffnungszeiten ist der Empfang stets besetzt
- ☒ Absicherung von Gebäudeschächten
- ☐ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☐ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner/Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

Zugang- und Zugriffskontrolle

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername/Passwort
- ☒ Gehäuseverriegelungen
- ☐ Sperren von externen Schnittstellen (USB)
- ☒ Verschlüsselung von Datenträgern in Laptops/Notebooks
- ☒ Erstellen von Benutzerprofilen
- ☐ Authentifikation mit biometrischen Verfahren
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☒ Einsatz einer Software-Firewall
- ☒ Einsatz einer Hardware-Firewall

☒ Einsatz von Anti-Viren-Software

☒ Einsatz von Intrustion-Detection-Systemen

☐ Einsatz einer Spyware & PUAs Software

☒ Erstellen eines Berechtigungskonzepts

☒ Anzahl der Administratoren auf das „Notwendigste" reduziert

☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☒ Physische Löschung von Datenträgern vor Wiederverwendung

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

☒ Verschlüsselung von Datenträgern

☒ Richtlinie „Clean Desk"

☒ Anleitung „Manuelle Desktopsperre"

☒ Mindestpasswortlängen und Passwortmanager

☐ Verschlüsselung von Smartphone Inhalten

☒ Verschlüsselung von mobilen Datenträgern

☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

☒ Verwaltung der Rechte durch Systemadministrator

☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☒ Sichere Aufbewahrung von Datenträgern

☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☐ Protokollierung der Vernichtung

☒ Angemessene Datenshredder (mind. Stufe P4)

☒ Stets aktuelle Softwareversionen

☒ Automatische Desktopsperre

Zweckbindungs-/Trennungskontrolle:

☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☒ Logische Mandantentrennung (softwareseitig)

☒ Erstellung eines Berechtigungskonzepts

☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

☒ Festlegung von Datenbankrechten

☐ Trennung von Produktiv- und Testsystem

Eingabekontrolle:

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten

☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten

☐ Sonstiges:

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle:

☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln

☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen

☒ E-Mail Verschlüsselung (S/MIME)

☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

☒ Verschlüsselung von Datenübertragungen nach Stand der Technik

☐ Verschlüsselung externer Datenträger bei Weitergabe (CDs, USB-Sticks etc.)

☒ Arbeitsanweisung an Mitarbeiter

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle:

☒ Unterbrechungsfreie Stromversorgung (USV)

☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

☐ Feuer- und Rauchmeldeanlagen

☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

☒ Testen von Datenwiederherstellung

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☐ In Hochwassergebieten: Serverräume über der Wassergrenze

☒ Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten

☒ Getrennte Partitionen für Betriebssysteme und Daten

☒ Incident-Response-Management

☐ Klimaanlage in Serverräumen

☒ Schutzsteckdosenleisten in Serverräumen

☒ Feuerlöschgeräte vor Serverräumen

☒ Erstellen und ständige Kontrolle eines Backup- & Recoverykonzepts

☒ Erstellen eines Notfallplans

☒ Serverräume nicht unter sanitären Anlagen

☒ Durchführung von Penettrationstests

☒ Regelmäßige Wartung der IT (Updates, Patches)

☒ Einsatz von Festplattenspiegelung

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

- ☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung
- ☒ Interner/Externer Datenschutzbeauftragter
- ☒ Software-Lösungen für Datenschutz-Management im Einsatz
- ☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- ☒ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
- ☒ Die Organisation kommt den Informationspflichten nach Art. 13, 14 DSGVO nach
- ☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- ☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt

Incident-Response-Management

- ☒ Dokumentation von Sicherheitsvorfällen und Datenpannen
- ☒ Einsatz von Virenscanner und regelmäßige Aktualisierung
- ☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
  ☒ Wurde den Beschäftigten schriftlich mitgeteilt
- ☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- ☒ Einbindung von DSB in Sicherheitsvorfälle und Datenpannen
- ☒ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ☒ Einsatz von Firewall und regelmäßige Aktualisierung

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- ☒ Privacy by default eingehalten
- ☒ Privacy bei Design eingehalten
- ☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Auftragskontrolle (Art. 28 DS-GVO):

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. Art. 28 ff. EU-DSGVO
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt (wenn erforderlich)
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- ☒ Vertragsstrafen bei Verstößen
- ☒ Regelung zum Einsatz weiterer Subunternehmer
- ☒ Kontrolle der Einhaltung bei Auftragnehmern
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit/Datengeheimnis
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung (Angemessenheitsbeschluss bzw. EU Standard-Vertragsklauseln)

Anlage 3 - Datenschutzbeauftragter

Datenschutzbeauftragter/-ansprechpartner des Auftragnehmers

secom IT GmbH

Adresse: Nienburger Str. 9a, 27232 Sulingen

Tel.: 04271 9473 800

E-Mail: datenschutz@secom-it.de

Anlage 4 – Unterauftragnehmer

Firmennamen	Kontaktdaten	Leistungserbringung
ecos GmbH & Co. KG	Mergenthalerallee 10-12 65760 Eschborn	Newsletterversand, Bearbeitung von Großanfragen über mehrere ecos Standorte, Verwalten von Telefonbucheinträgen bei der Dt. Telekom, Verwaltung der E-Mail-Accounts
Partner-Business Center (der ecosGruppe angeschlossene Center)	siehe Website www.ecos-office.com/de/standorte/	Je nach gebuchter Leistung durch den Auftraggeber.
GesMIT mbH	Bruchbrunnenstraße 19 66123 Saarbrücken	Bereitstellung, Support und Wartung für Telefonmanagementsystem sowie SMS- bzw. Telefaxversand
Locaboo GmbH	Balanstr. 73 | Haus 12 81541 München	Raumplanung
LIONWARE GmbH	Isestraße 123 20149 Hamburg	Identitätsprüfung
microPLAN IT-Systemhaus GmbH	Spatzenweg 2 48282 Emsdetten	Wartung und Pflege der Telefonanlage
ZDS Bürosysteme Vertrieb & Service GmbH	Schlattgrabenstraße 24 72141 Walddorfhäslach	Wartung und Pflege für Büro Druck- und Scanlösungen
Systempartner Stuttgart IT-Service GmbH	Schulze-Delitzsch-Straße 41 70565 Stuttgart	Wartung und Pflege der sonstigen IT-Systeme
Tedesco Dienstleistungen	Taunusstraße 54 71032 Böblingen	Gebäude- und Büroreinigung mit Mülltrennung und Müllentsorgung