Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen

DATA Security GmbH
Carl-Jordan-Straße 14
83059 Kolbermoor
(nachfolgend: „DATA Security GmbH“)

und

Nutzer DATA Security Manager / Compliance / Verfahrensdoku / Hinweisgebersystem
(nachfolgend: „Kunde“)

Präambel

Die DATA Security GmbH ist Anbieter von Lösungen im Bereich IT und Compliance.
Für die Nutzung von DATA Security GmbH Lösungen und Inanspruchnahme von Dienstleistungen besteht ein Hauptvertrag zwischen der DATA Security GmbH und dem Kunden. Im Hauptvertrag sind die jeweiligen Rechte und Pflichten geregelt. Darüber hinaus gelten die Geschäftsbedingungen der DATA Security GmbH, die dem Hauptvertrag als Anhang beigefügt sind. Mit diesem Vertrag sollen zusätzlich die Vorgaben der DS-GVO hinsichtlich Art. 28 DS-GVO geregelt werden.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand
DATA Security GmbH verarbeitet personenbezogene Daten im Auftrag des Kunden entsprechend seiner Weisung. Die Verarbeitung umfasst alle Tätigkeiten, die im Hauptvertrag geregelt sind. Der Hauptvertrag und die Geschäftsbedingungen von DATA Security GmbH sind Bestandteil dieses Vertrags.

(2) Dauer
Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des bestehenden Hauptvertrags für die Nutzung von DATA Security GmbH Lösungen und Inanspruchnahme von Dienstleistungen.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten durch die DATA Security GmbH für den Kunden sind konkret beschrieben im Hauptvertrag die Nutzung von DATA Security GmbH Lösungen und Inanspruchnahme von Dienstleistungen. 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 darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Für den Fall einer Verarbeitung in einem Drittland wird das angemessene Schutzniveau durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO) sichergestellt. Zusätzlich können Garantien, die Art.46 EU-DS-GVO vorsieht, abgeschlossen werden.

(2) Art der Daten
Alle Arten von personenbezogenen Daten, die DATA Security GmbH im Auftrag des Kunden verarbeitet. Das sind insbesondere folgende Kategorien:

- Stammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Risiken hinsichtlich GwG
- Daten höherer Kategorien
- Vertragsdaten

Bei Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO ist der Kunde verpflichtet, selbst dafür Sorge zu tragen (in eigener Verantwortung), dass hierzu alle relevanten gesetzlichen Vorgaben eingehalten werden.

(3) Kategorien betroffener Personen
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitarbeiter und Familienangehörige
- Dienstleister und deren Mitarbeiter
- Geschäftspartner und deren Mitarbeiter
- Kunden/Mandanten und deren Geschäftspartner/Mitarbeiter
- Ggf. andere Personen

3. Technisch-organisatorische Maßnahmen

(1) Die DATA Security GmbH 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 Kunden zur Prüfung zu übergeben. Bei Akzeptanz durch den Kunden werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Kunden einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Die DATA Security GmbH hat die Sicherheit gem. Art. 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 (Siehe Anlage 1).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der DATA Security GmbH 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) Die DATA Security GmbH darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die DATA Security GmbH wendet, wird die DATA Security GmbH dieses Ersuchen unverzüglich an den Kunden weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Kunden unmittelbar durch die DATA Security GmbH sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten der DATA Security GmbH

(1) Die DATA Security GmbH 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) Die DATA Security GmbH ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner der DATA Security GmbH wird Herr Dominik Mikulovic, Geschäftsführer, +49 8031 2300100, info@data-security.one benannt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Die DATA Security GmbH 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.

c) Die DATA Security GmbH und jede der DATA Security GmbH unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Kunden verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

d) 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 (Siehe Anlage 1).

e) Der Kunde und die DATA Security GmbH arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

f) Die unverzügliche Information des Kunden 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 bei der DATA Security GmbH ermittelt.

g) Soweit der Kunde 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 ausgesetzt ist, hat ihn die DATA Security GmbH nach besten Kräften zu unterstützen.

h) Der Kunde 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.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kunden 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 DATA Security GmbH 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. Die DATA Security GmbH 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 Kunde erteilt der DATA Security GmbH die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DS-GVO in Anspruch zu nehmen.

(3) Die jeweils aktuell eingesetzten, weiteren Auftragsverarbeiter kann der Auftraggeber unter: https://data-security.one/wp-content/uploads/Liste_der_Dienstleister.pdf abrufen. Diese Liste wird, falls sich Änderungen ergeben, quartalsweise aktualisiert.

(4) Die DATA Security GmbH informiert den Kunden, wenn eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt wird. Die Änderungen kann der Auftraggeber unter: https://data-security.one/wp-content/uploads/Liste_der_Dienstleister.pdf abrufen. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.

(5) Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrechtlichen Grund erhoben werden. Der Einspruch ist innerhalb von 4 Wochen nach Bereitstellung der Information gegenüber DATA Security GmbH in Schriftform zu erheben. Im Fall eines begründeten Einspruchs kann DATA Security GmbH nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung der DATA Security GmbH nicht zumutbar ist - die von der Änderung betroffene Leistung oder den gesamten Vertrag gegenüber dem Kunden innerhalb von 4 Wochen nach Zugang des Einspruchs kündigen.

(6) Erteilt DATA Security Aufträge an Subunternehmer, so obliegt es der DATA Security GmbH, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Die volle Verantwortung für die von DATA Security eingeschalteten Subunternehmer bleibt bei der DATA Security GmbH.

7. Kontrollrechte des Kunden

(1) Der Kunde hat das Recht, im Benehmen mit der DATA Security GmbH 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 der DATA Security GmbH in dessen Geschäftsbetrieb zu überzeugen.

(2) Die DATA Security GmbH stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten der DATA Security GmbH nach Art. 28 DS-GVO überzeugen kann. Die DATA Security GmbH verpflichtet sich, dem Kunden 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;
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Kunden kann die DATA Security GmbH einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen der DATA Security GmbH

(1) Die DATA Security GmbH unterstützt den Kunden 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 Kunden zu melden
c) die Verpflichtung, dem Kunden 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 Kunden für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Kunden im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten der DATA Security GmbH zurückzuführen ist, kann die DATA Security GmbH eine Vergütung beanspruchen.

9. Weisungsbefugnis des Kunden

(1) Mündliche Weisungen bestätigt der Kunde unverzüglich (mind. Textform).

(2) Die DATA Security GmbH hat den Kunden unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften.

(3) Die DATA Security GmbH ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Kunden 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 Kunden – spätestens mit Beendigung der Leistungsvereinbarung – hat die DATA Security GmbH sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kunden 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 die DATA Security GmbH entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Kunden übergeben.

Anlage 1: Technisch und organisatorische Maßnahmen (TOM)

Technische und organisatorische Maßnahmen (TOM)
i.S.d. Art. 32 DS-GVO
DATA Security GmbH, Carl-Jordan-Straße 14, 83059 Kolbermoor

Unternehmen, die selbst oder als Dienstleister (nach Art. 28 DS-GVO) personenbezogene Daten erheben, verarbeiten oder Zugriff darauf haben, müssen technische und organisatorische Maßnahmen treffen und umsetzen, welche die Einhaltung der Datenschutzgrundsätze, sowie die Sicherheit der Verarbeitung (z.B. nach BSI-Richtlinie) personenbezogener Daten gewährleisten.

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

a) Technische Maßnahmen
- Manuelles Schließsystem
- Sicherheitsschlösser
- Klingelanlage

b) Organisatorische Maßnahmen
- Schlüsselregelung / Liste
- Empfang
- Besucher in Begleitung durch Mitarbeiter
- Sorgfalt bei Auswahl Reinigungsdienste
- Ansprache unbekannter Personen
- Begrenzung der Bereiche, die externe Dienstleister (z.B. Reinigungs- und Wartungspersonal) aufsuchen können

2. Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten verwendet werden können.

a) Technische Maßnahmen
- Login mit Benutzername + Passwort
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung von Datenträgern
- Automatische Desktopsperre
- Verschlüsselung von Notebooks/Tablets

b) Organisatorische Maßnahmen
- Verwalten von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortvergabe
- Personenkontrolle beim Empfang
- Richtlinie „Sicheres Passwort“
- Richtlinie „Clean Desk“

- Allg. Richtlinie Datenschutz und Sicherheit
- Mobile Device Policy
- Anleitung „Manuelle Desktopsperre“

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und die personenbezogenen Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt verwendet werden können.

a) Technische Maßnahmen
   - Akten Schredder (mind. Stufe 3, cross cut)
   - Externer Aktenvernichter (DIN 32757)
   - Physische Löschung von Datenträgern
   - Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
   - Verschlüsselung von Datenträgern

b) Organisatorische Maßnahmen
   - Einsatz Berechtigungskonzepte
   - Verwaltung der Rechte durch einen Systemadministrator
   - Minimale Anzahl an Administratoren
   - Protokollierung der Vernichtung von Datenträgern

4. 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.

a) Technische Maßnahmen
   - E-Mail-Verschlüsselung
   - Einsatz von VPN
   - Protokollierung der Zugriffe und Abrufe
   - Bereitstellung über verschlüsselte Verbindungen wie sftp, https

b) Organisatorische Maßnahmen
   - Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen

5. 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.

a) Technische Maßnahmen
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatisierte Kontrolle der Protokolle

b) Organisatorische Maßnahmen
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Klare Zuständigkeit für Löschungen

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können.

a) Organisatorische Maßnahmen
- Vorherige Prüfung der von Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

7. Verfügbarkeitskontrolle

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

a) Technische Maßnahmen
- Feuer- und Rauchmeldeanlagen inkl. Feuerlöscher Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Serverraum klimatisiert
- USV
- Schutzsteckdosenleisten Serverraum
- RAID- System/ Festplattenspiegelung
- Videoüberwachung Serverraum
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum

b) Organisatorische Maßnahmen
- Backup & Recovery-Konzept

- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Getrennte Partitionen für Betriebssysteme und Daten

8. Trennungskontrolle (Trennungsgebot)

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

a) Technische Maßnahmen
   - Trennung von Produktiv- und Testumgebung
   - Physikalische Trennung (Systeme/Datenbanken/Datenträger)
   - Logische Mandantentrennung (softwareseitig)

b) Organisatorische Maßnahmen
   - Steuerung über Berechtigungskonzept
   - Festlegung von Datenbankrechten

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

Datenschutz-Management (Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.)

- Regelmäßige Schulung der Mitarbeiter zum Datenschutz
- Ein Verzeichnis der Verarbeitungstätigkeiten ist vorhanden, vollständig und aktuell.
- Es bestehen Standards für die IT-Sicherheit
- Die Aufbewahrung der elektronischen Protokolle ist geregelt
- Es gibt Regelungen über die Sicherung des Datenbestands
- Nachweise über die Verpflichtung auf das Datengeheimnis sind vorhanden
- Ein Datenschutzkonzept ist vorhanden
- Datenschutz- und Datensicherungsmaßnahmen werden gelegentlich unvermutet kontrolliert

Incident-Response-Management (Maßnahmen, die gewährleisten, dass im Falle einer Datenpanne eine unmittelbare Information an den Auftraggeber erfolgt.)

- Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne
- Es existiert ein internes Incident-Response-Management-Konzept
- Es gibt ein Konzept zur Meldung von Daten-pannen an den Auftraggeber

DATA Security GmbH
Carl-Jordan-Straße 14
83059 Kolbermoor

+49 (0) 8031 2 300 100
info@data-security.one
www.data-security.one

Handelsregister Traunstein HRB26792
Geschäftsführer: Dominik Mikulovic