Vertrag zur Auftragsverarbeitung

zwischen

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ
(nachfolgend: „DATA Security“)

und

Anwender von DATA Security Manager
(nachfolgend: „Kunde“)

Stand: Juli 2022

Präambel
DATA Security AG ist Anbieter von Lösungen im Bereich IT und Compliance.
Für die Nutzung von DATA Security Lösungen und Inanspruchnahme von Dienstleistungen besteht ein Hauptvertrag zwischen dem Auftraggeber und Auftragnehmer. Im Hauptvertrag sind die jeweiligen Rechte und Pflichten geregelt. Darüber hinaus gelten die Geschäftsbedingungen der DATA Security, 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 verarbeitet personenbezogene Daten im Auftrag des Kunden (Auftragsgebers) entsprechend seiner Weisung. Die Verarbeitung umfasst alle Tätigkeiten, die im Hauptvertrag geregelt sind. Der Hauptvertrag und die Geschäftsbedingungen von DATA Security sind Bestandteil dieses Vertrags.

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

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Hauptvertrag die Nutzung von DATA Security 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-DSGVO vorsieht, abgeschlossen werden.

(2) Art der Daten
Alle Arten personenbezogener Daten, die DATA Security im Auftrag des Kunden (Auftraggebers) 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 (Auftraggeber) 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) 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. 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).

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

(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.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) 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 ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr Slobodan Mikulovic, +41 44 777 79 59, info@data-security.ch benannt.
   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.
   c) 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.
   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 Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
   f) 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.
   g) 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.
   h) 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.

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

i) 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 Auftraggeber erteilt dem Auftragnehmer 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.ch/upload/public-docs/Liste%20DL/Liste%20der%20Dienstleister%20.pdf abrufen. Diese Liste wird, falls sich Änderungen ergeben, quartalsweise aktualisiert.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Die volle Verantwortung für die vom Auftragnehmer eingeschalteten Subunternehmer bleibt beim Auftragnehmer.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende 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;
- 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.

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

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, 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 unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Datenschutzvorschriften.

(3) Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

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 den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

Anlage 1: Technisch und organisatorische Massnahmen (TOM)

Technische und organisatorische Massnahmen (TOM)

i.S.d. Art. 32 DSGVO

DATA Security AG, Färberstrasse 9, 8832 Wollerau SZ

Unternehmen, die selbst oder als Dienstleister (nach Art. 28 DSGVO) 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.

Technische Massnahmen

- Manuelles Schliesssystem
- Sicherheitsschlösser
- Klingelanlage

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.

Technische Massnahmen

- Login mit Benutzername + Passwort
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall
- Einsatz VPN bei Remote-Zugriffen
- Verschlüsselung von Datenträgern

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

- Automatische Desktopsperre
- Verschlüsselung von Notebooks/Tablets

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.

Technische Massnahmen
- Aktenschredder (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

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.

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

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

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.

Massnahmen

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

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 Auftraggebers verarbeitet werden können.

Organisatorische Massnahmen

- Vorherige Prüfung der vom 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.

Technische Massnahmen

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher Serverraum
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Serverraum klimatisiert
- USV

DATA Security AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939

- Schutzsteckdosenleisten Serverraum
- RAID- System/ Festplattenspiegelung
  Videoüberwachung Serverraum
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum

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.

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

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 AG
Färberstrasse 9
8832 Wollerau SZ

www.data-security.ch
info@data-security.ch
+41 44 777 79 59

CEO Slobodan Mikulovic
UID: CHE-327.210.939