Vereinbarung über die Auftragsdatenbearbeitung

Vorbemerkungen

Die vorliegende Vereinbarung (**Vereinbarung**) konkretisiert die Verpflichtungen des Kunden und des Auftragsbearbeiters (zusammen die Parteien) in Bezug auf die Vorgaben aus dem Schweizer Datenschutzgesetz (**DSG**) und der Datenschutz-Grundverordnung der EU (**EU-DSGVO**). Sie ergänzt diesbezüglich die vertraglichen Vereinbarungen über die Dienstleistungen des Auftragsbearbeiters an den Kunden. Es kann sich dabei um einen einzelnen oder mehrere Verträge zwischen dem Auftragsbearbeiter und dem Kunden handeln (**Vertrag**).

Die Vereinbarung gilt insofern und insoweit als die nachfolgenden Voraussetzungen erfüllt sind:

(a) Der Kunde tritt entweder als Verantwortlicher oder Auftragsbearbeiter im Anwendungsbereich des DSG und/oder der EU-DSGVO auf und

(b) der Kunde zieht DAUF AG im Rahmen des Vertrags als Auftragsbearbeiter oder Unter-Auftragsbearbeiter für die Bearbeitung von Personendaten bzw. personenbezogenen Daten bei, welche vom Anwendungsbereich des DSG und/oder der EU-DSGVO erfasst sind (**Personendaten**).

1. Gegenstand, Art, Zweck und Dauer der Datenbearbeitung

Der Gegenstand der Datenbearbeitung, ihre Art, ihr Zweck und ihre Dauer ergeben sich aus dem Vertrag. Die Kategorien der bearbeiteten Personendaten, die Kategorien der von der Datenbearbeitung betroffenen Personen und die zu treffenden technischen und organisatorischen Massnahmen (TOM) werden im Vertrag und/oder in den Anhängen 1 und 2 zu dieser Vereinbarung beschrieben.

Soweit der Auftragsbearbeiter im Laufe der weiteren Zusammenarbeit weitere Dienstleistungen für den Kunden übernimmt, gilt diese Vereinbarung auch für diese Dienstleistungen.

2. Weisungen

(a) Befolgung von Weisungen: Der Auftragsbearbeiter ist verpflichtet, die Personendaten ausschliesslich gemäss den Bestimmungen des Vertrags und dieser Vereinbarung zu bearbeiten und bei ihrer Bearbeitung den Weisungen des Kunden zu folgen. Vorbehalten sind abweichende Pflichten des anwendbaren Rechts (z.B. gesetzliche Pflichten oder verbindliche Anordnungen zuständiger Behörden).

(b) Rechtmässigkeit der Datenbearbeitung: Der Kunde ist für die Rechtmässigkeit der Datenbearbeitung an sich, inklusive der Zulässigkeit der Auftrags-/Unter-Auftragsbearbeitung verantwortlich.

(c) Erteilung von Weisungen: Die Weisungen des Kunden sind im Vertrag und durch diese Vereinbarung dokumentiert. Der Kunde darf dem Auftragsbearbeiter jederzeit schriftlich darüberhinausgehende Weisungen erteilen. Solche Einzelweisungen bedürfen einer vorherigen Zustimmung des Auftragsbearbeiters und sind zu dokumentieren. Der Auftragsbearbeiter stimmt diesen Weisungen zu, soweit sie im Rahmen der im Vertrag vereinbarten Dienstleistungen umsetzbar und zumutbar sind. Führen solche Weisungen zu Mehrkosten für den Auftragsbearbeiter oder einem geänderten Leistungsumfang, so ist das Änderungsverfahren gemäss Vertrag anwendbar.

(d) Zulässigkeit von Weisungen: Der Auftragsbearbeiter informiert den Kunden unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen das DSG oder die EU-DSGVO verstösst. In diesem Fall darf der Auftragsbearbeiter die Umsetzung der Weisung aussetzen, bis sie vom Kunden bestätigt oder geändert wurde. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemässe Bearbeitung der Personendaten beim Kunden liegt. Der Auftragsbearbeiter darf jederzeit davon ausgehen, dass Weisungen des Kunden betreffend Zugriffsberechtigungen auf Personendaten oder deren Herausgabe an ihn gesetzeskonform sind.

3. Weitere Pflichten des Auftragsbearbeiters

(a) Zweckbindung: Der Auftragsbearbeiter bearbeitet die Personendaten ausschliesslich zum Zweck der Vertragserfüllung und gemäss den im Vertrag und dieser Vereinbarung vereinbarten Regelungen. Dem Auftragsbearbeiter bleibt es vorbehalten, die Personendaten zu anonymisieren oder zu aggregieren, sodass eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist, und in dieser Form zum Zweck der bedarfsgerechten Gestaltung, der Weiterentwicklung und der Optimierung sowie der Erbringung des nach Massgabe des Vertrags vereinbarten Dienstes zu verwenden.

(b) Technische und organisatorische Massnahmen (TOM): Der Auftragsbearbeiter ergreift angemessene, in jedem Fall aber mindestens die in Anhang 2 umschriebenen TOM zum Schutz der Personendaten. Der Auftragsbearbeiter ist während der Dauer der Vereinbarung berechtigt, die TOM anzupassen, sofern dabei das Sicherheitsniveau nicht abgesenkt wird. Im Widerspruchsfall gehen im Vertrag geregelte spezifischere TOM denjenigen gemäss Anhang 2 vor.

(c) Verzeichnis über die Datenbearbeitungen: Der Auftragsbearbeiter führt ein den Anforderungen gemäss Art. 12 Abs. 1 DSG bzw. Art. 30 Abs. 2 EU-DSGVO entsprechendes Verzeichnis über seine Bearbeitung von Personendaten. Der Auftragsbearbeiter gewährt dem Kunden auf Anfrage Einblick in diejenigen Teile des Bearbeitungsverzeichnisses, die die Bearbeitung von Personendaten betreffen, die für die an ihn erbrachten Dienstleistungen relevant sind.

(d) Vertraulichkeit und Verschwiegenheit: Der Auftragsbearbeiter stellt sicher, dass es den mit der Bearbeitung der Personendaten befassten Personen untersagt ist, diese zu anderen als den vereinbarten Zwecken und abweichend zu dieser Vereinbarung zu bearbeiten. Er stellt zudem sicher, dass alle Personen mit Zugang zu den Personendaten einer gesetzlichen oder vertraglichen Vertraulichkeits-/Verschwiegenheitspflicht unterstehen. Soweit die bearbeiteten Personendaten dem Berufsgeheimnis unterstehen, handelt der Auftragsbearbeiter als Hilfsperson und erfüllt die anwendbaren gesetzlichen Verpflichtungen.

(e) Meldung von Sicherheitsverletzungen: Bei konkret vermuteten und bei festgestellten Sicherheitsverletzungen beim Auftragsbearbeiter oder einem Unterauftragsbearbeiter, die – ob rechts-, vertrags- oder weisungswidrig oder unbeabsichtigt – zur Vernichtung, zum Verlust, zur Veränderung oder zur Offenlegung von Personendaten führen, informiert der Auftragsbearbeiter den Kunden so rasch als möglich in angemessener Weise über Art und Ausmass der Verletzung sowie mögliche Abhilfemassnahmen. Die Parteien treffen in so einem Fall die erforderlichen Massnahmen zur Sicherstellung des Schutzes der Personendaten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen sowie die Parteien und sprechen sich hierzu unverzüglich ab.

(f) Unterstützungspflichten:

(i) Soweit sich eine betroffene Person im Zusammenhang mit datenschutzrechtlichen Ansprüchen (z.B. mit einem Berichtigungs-, Auskunfts- oder Löschbegehren) an den Auftragsbearbeiter wendet, leitet der Auftragsbearbeiter das entsprechende Begehren unverzüglich an den Kunden weiter. Er unterstützt den Kunden angemessen bei der Bearbeitung solcher Begehren. Der Auftragsbearbeiter kann bei grösseren Aufwänden eine vorgängig zu vereinbarende separate Vergütung verlangen.

(ii) Der Auftragsbearbeiter unterstützt den Kunden bei der Durchführung einer Datenschutz-Folgenabschätzung, Konsultationen der Aufsichtsbehörde, Meldungen an diese und ähnliches mit notwendigen Daten und Informationen. Der Auftragsbearbeiter kann bei grösseren Aufwänden eine vorgängig zu vereinbarende separate Vergütung verlangen.

(g) Rückgabe- und Löschpflicht:

(i) Personendaten sind nach Vertragsende gemäss den vertraglichen Bestimmungen oder gemäss den Weisungen des Kunden herauszugeben oder zu löschen, sofern nicht gesetzlich eine Verpflichtung des Auftragsbearbeiters zur weiteren Aufbewahrung der Personendaten besteht. Der Auftragsbearbeiter setzt für die Löschung von Personendaten branchenübliche Verfahren ein.

(ii) Dokumentationen, die dem Nachweis der auftragsgemässen Bearbeitung von Personendaten dienen, dürfen durch den Auftragsbearbeiter auch nach Beendigung der Vereinbarung im Einklang mit den gesetzlichen Vorgaben aufbewahrt werden.

4. Pflichten und Obliegenheiten des Kunden

(a) Regulatorische Pflichten: Der Kunde erfüllt sämtliche auf seine Rolle als Bearbeiter von Personendaten anwendbaren regulatorischen Pflichten. Er ist für die Rechtmässigkeit der Bearbeitung der Personendaten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Soweit der Kunde seinerseits als Auftragsbearbeiter eines Verantwortlichen tätig ist, ist der Auftragsbearbeiter ein Unterauftragsbearbeiter. In diesem Fall sichert der Kunde mit jeder Weisung zu, dass es sich um die Weisung des Verantwortlichen handelt. Sollten Dritte gegen den Auftragsbearbeiter aufgrund der Bearbeitung von Personendaten nach Massgabe dieser Vereinbarung Ansprüche geltend machen, wird der Kunde den Auftragsbearbeiter von allen solchen Ansprüchen freistellen.

(b) Technische und organisatorische Massnahmen (TOM): Der Kunde trifft in seinem Verantwortungsbereich (z.B. seinen Systemen und Gebäuden) selbst angemessene technische und organisatorische Massnahmen zum Schutz der Personendaten.

(c) Informationspflichten:

(i) Der Kunde informiert den Auftragsbearbeiter unverzüglich, wenn er in der Leistungserbringung des Auftragsbearbeiters eine Datenschutzverletzung feststellt.

(ii) Ist der Auftragsbearbeiter gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Bearbeitung von Personendaten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Kunde verpflichtet, den Auftragsbearbeiter bei der Erfüllung dieser Verpflichtungen zu unterstützen.

5. Kontakt

(a) Kunde: Kontaktperson ersichtlich im Vertrag zwischen Kunde und DAUF AG

(b) Auftragsbearbeiter: DAUF AG, Via Figino 6, 6917 Barbengo, dataprotection@dauf.ch

6. Unterauftragsbearbeiter

(a) Beizugsrecht: Sofern der Vertrag keine einschränkenden Bestimmungen zum Beizug von Dritten beinhaltet, ist der Auftragsbearbeiter befugt, Unterauftragsbearbeiter beizuziehen. Dies, sofern der Auftragsbearbeiter mit dem Unterauftragsbearbeiter eine Vereinbarung trifft, um die Einhaltung der Verpflichtungen gemäss der vorliegenden Vereinbarung sicherzustellen.

(b) Genehmigung: Eine Liste der bei Vertragsbeginn bestehenden und hiermit genehmigten Unterauftragsbearbeiter mit Zugriff auf Personendaten findet sich in Anhang 3. Der Auftragsbearbeiter informiert den Kunden über beabsichtigte Änderungen. Innerhalb eines Monats nach der Benachrichtigung durch den Auftragsbearbeiter kann der Kunde Einspruch erheben, wenn wichtige datenschutzrechtliche Gründe gegen den Beizug des betroffenen Unterauftragsbearbeiters sprechen. Der Einspruch durch den Kunden muss schriftlich erfolgen und die Gründe für den Einspruch beinhalten. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösung zwischen den Parteien nicht möglich, so wird dem Kunden in Bezug auf die vom Wechsel des Unterauftragsbearbeiters betroffene Dienstleistung ein Kündigungsrecht eingeräumt.

7. Ort der Datenbearbeitung

Jedwede Bekanntgabe von Personendaten durch den Auftragsbearbeiter ins Ausland oder an eine internationale Organisation ist nur zulässig, wenn der Auftragsbearbeiter die Bestimmungen von Art. 16 ff. DSG bzw. von Kapitel V EU-DSGVO einhält. Soweit hingegen eine solche Bekanntgabe von Personendaten vom Kunden gewünscht ist bzw. in seinem Auftrag erfolgt, obliegt die Einhaltung der entsprechenden Bestimmungen ausschliesslich dem Kunden.

8. Prüfrechte

(a) Prüfrecht: Der Auftragsbearbeiter ist verpflichtet, dem Kunden auf Verlangen Informationen zur Verfügung zu stellen, um die Einhaltung der vereinbarten Pflichten zu dokumentieren. Der Kunde hat das Recht, die Einhaltung der Pflichten gemäss dieser Vereinbarung durch den Auftragsbearbeiter zu prüfen. Der Auftragsbearbeiter ist verpflichtet, bei Prüfungen jeweils angemessen mitzuwirken. Der Kunde nimmt bei der Planung und Durchführung der Prüfung Rücksicht auf die Bedürfnisse und Sicherheitsanforderungen des Auftragsbearbeiters und hat Vertraulichkeitspflichten des Auftragsbearbeiters zu respektieren.

(b) Externe Prüfstelle: Der Kunde hat das Recht, die Prüfung nach Ziff. 8(a) durch eine externe, fachkundige und zur Vertraulichkeit verpflichtete Stelle durchführen zu lassen. Die beim Kunden anfallenden Kosten der Prüfung trägt der Kunde selbst.

(c) Korrekturmassnahmen: Wurden im Rahmen der Prüfung Verletzungen dieser Vereinbarung festgestellt und nachgewiesen, so nimmt der Auftragsbearbeiter unverzüglich geeignete Korrekturmassnahmen vor.

9. Schlussbestimmungen

(a) Umfang: Die Parteien regeln in der Vereinbarung nur das datenschutzrechtliche Auftragsbearbeitungsverhältnis. Sie beabsichtigen nicht den in der Leistungsvereinbarung vereinbarten Leistungskatalog auszuweiten oder einzuschränken.

(b) Haftung: Für die Haftung aus Verletzungen dieser Vereinbarung gelten die für die Dienstleistungen vereinbarten oder von Gesetzes wegen geltenden Haftungsregelungen. Der Kunde verpflichtet sich, den Auftragsbearbeiter auch von allen etwaigen Geldbussen, die gegen den Auftragsbearbeiter verhängt werden, in dem Umfang freizustellen, in dem der Kunde Anteil an der Verantwortung für den durch die Geldbusse sanktionierten Verstoss trägt.

(c) Laufzeit: Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit aller Verträge zwischen dem Auftragsbearbeiter und dem Kunden, unter welchen der Auftragsbearbeiter für den Kunden Personendaten bearbeitet, sofern sich aus dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

(d) Mitteilungen: In dieser Vereinbarung vorgesehene Mitteilungen müssen jeweils ausdrücklich und in Textform (z.B. per E-Mail oder Post) erfolgen, sofern nichts anderes vereinbart ist.

(e) Änderungen und Ergänzungen: In Abweichung allfälliger Schriftformvorbehalte im Vertrag kann die vorliegende Vereinbarung auch auf elektronischem Weg zwischen den Parteien vereinbart oder geändert werden.

(f) Streitschlichtung: Das anwendbare Recht und der Gerichtsstand richten sich nach dem Vertrag. Der Kunde bleibt aber berechtigt, vor jedem zuständigen Gericht vorsorgliche Massnahmen zu verlangen und seine Ansprüche gegen den Auftragsbearbeiter im Fall einer Inanspruchnahme durch einen Dritten vor dem Gericht der Hauptklage geltend zu machen.

(g) Konfliktregelung: Sofern der Vertrag oder spezialgesetzliche Vorgaben nicht strengere oder weitergehende Bestimmungen enthalten, geht diese Vereinbarung bei Widersprüchen dem Vertrag vor. Im Übrigen gelten die Regelungen des Vertrages einschliesslich weiterer Datenschutz- und Sicherheitsbestimmungen unverändert fort.

Anhang 1: Konkretisierung der ADV

1. Arten von Personendaten

Die Auftragsdatenbearbeitung kann insbesondere folgende Kategorien von Personendaten umfassen:

a. *Stammdaten* (Daten, die sich direkt auf die Person und ihre Eigenschaften beziehen; z.B. Vorname, Name, Geburtsdatum, Alter, Geschlecht, Nationalität, AHV-Nummer, Familienstand, Angaben zum Berufsprofil und der Beschäftigung, Kundenhistorie etc.)
b. *Gesundheitsdaten* (Daten über den Gesundheitszustand einer Person; z.B. Diagnosen, Therapieformen, behandelnder Arzt etc.)
c. *Vertragsdaten* (Daten, die im Zusammenhang mit dem Vertragsschluss bzw. der Vertragsabwicklung anfallen; z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse, Abrechnungs- und Zahlungsdaten etc.)
d. *Kommunikationsdaten* (z.B. E-Mail-Adresse, Telefonnummer, Adresse, Inhalt der Korrespondenz, Randdaten etc.)
e. *Technische Daten und Benutzerinformationen* (Daten, die im Zusammenhang mit der Verwendung der Website oder Applikation anfallen, z.B. IP-Adresse, Login-Daten, Kundennummer, Personalnummer etc.)
f. *Verhaltensdaten* (z.B. Daten über die Nutzung von Websites, Informationen über die Verwendung elektronischer Mitteilungen)
g. *Präferenzdaten* (Daten, welche über Bedürfnisse, Interessen, Präferenzen, Eigenschaften oder voraussichtliches Verhalten Aufschluss geben)
h. *Sonstige Daten* (z.B. Daten im Zusammenhang mit behördlichen oder gerichtlichen Verfahren, im Rahmen von Schutzkonzepten, Fotos, Videos und Tonaufnahmen, Registrierungsdaten)

2. Besonders schützenswerte Personendaten

Bei diesen Daten handelt es sich um Personendaten, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten sowie Daten über die Intimsphäre.

3. Geheimnisgebundene Daten

Bei diesen Daten kann es sich beispielsweise um das Berufsgeheimnis, sowie die Verschwiegenheitspflicht gemäss Sozialversicherungsrecht unterliegende Daten handeln.

4. Betroffene Personen

Von der Auftragsdatenbearbeitung können insbesondere folgende Kategorien von Personen betroffen sein:

a. Aktuelle, ehemalige und potenzielle Endkunden, Apotheken, Drogerien, Altersheime und Diverse
b. Aktuelle, ehemalige und potenzielle Mitarbeitende und andere Hilfspersonen des Kunden
c. Geschäftspartner, Verkäufer, Lieferanten, Berater, Vertreter des Kunden, die natürliche Personen sind sowie deren Mitarbeitende

Anhang 2: Technische und organisatorische Massnahmen

In diesem Anhang werden die technischen und organisatorischen Massnahmen beschrieben, welche der Auftragsbearbeiter ergreift, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Massnahmen sind generisch zu verstehen und kommen jeweils dann zur Anwendung, wenn im Vertrag nichts Abweichendes definiert ist. Findet die Datenbearbeitung durch vom Auftragsbearbeiter beigezogene Unterauftragsbearbeiter statt, sorgt der Auftragsbearbeiter mittels geeigneter vertraglicher Vereinbarungen dafür, dass die Unterauftragsbearbeiter vergleichbare Massnahmen einhalten.

Die Beurteilung, ob die nachfolgend beschriebenen technischen und organisatorischen Massnahmen zum Schutz der dem Auftragsbearbeiter anvertrauten Daten (namentlich bei besonders schützenswerten Personendaten oder geheimnisgebundenen Daten) angemessen sind, obliegt ausschliesslich dem Kunden.

Zutrittskontrolle:

- Die Flächen sind in verschieden stark gesicherte Sicherheitszonen unterteilt. Öffentliche Zonen sind für jedermann zugänglich. Um in gesicherte Zonen Zutritt zu erhalten, wird ein Badge, Schlüssel oder dergleichen benötigt. Bei der Nutzung von Badges sind diese grundsätzlich zu personalisieren. Sind nicht personalisierte Badges im Einsatz, wird über die temporären Besitzer Protokoll geführt. Die Ausgabe von Schlüsseln oder dergleichen an die berechtigten Personen wird ebenfalls protokolliert. Das Verfahren zur Ausgabe von Badges, Schlüsseln oder dergleichen wird in entsprechenden Dokumenten geregelt. Besucher müssen sich registrieren und werden in den gesicherten Zonen von den verantwortlichen Mitarbeitern begleitet.
- Die Rechenzentren verfügen über die nötigen physischen Schutzmassnahmen, um einen unberechtigten Zugang zeitnah zu erkennen und einen entsprechenden Alarm auszulösen.
- Die Rechenzentren verfügen über die weiteren nötigen Schutzmassnahmen, um Gefahren durch Naturereignisse wie Blitz, Regen, Überschwemmung etc. möglichst so stark zu reduzieren, dass diese nicht mehr relevant für den Rechenzentrumsbetrieb sind.
- Falls für Dienstleistungen Rechenzentren von Dritten für die permanente Speicherung von Daten genutzt werden, wird sichergestellt, dass die Betreiber eines solchen Rechenzentrums vergleichbare Bedingungen und damit ein äquivalentes Sicherheitsniveau erfüllen.
- Die Rechenzentren können mit Video überwacht werden. Die Aufbewahrungsfrist und der Zugriff auf die Aufnahmen sind festgelegt.
- Im Falle, dass der Kunde seine Daten bei sich vor Ort speichert, kann DAUF AG Empfehlungen abgeben, wie diese Räume zu sichern sind. Es liegt in der Verantwortung des Kunden, die nötigen Schutzmassnahmen zu treffen.
- Es erfolgt eine sorgfältige Auswahl des Personals.
- Neue Mitarbeitende werden bei ihrem Arbeitsbeginn mit den relevanten Regeln zur eigenen Sicherheit und zur Datensicherheit vertraut gemacht.
- Bestehende Mitarbeitende werden regelmässig zum sorgfältigen Umgang mit Daten geschult und auf Sicherheitsrisiken aufmerksam gemacht.

- Wenn Mitarbeitende die DAUF AG verlassen, wird die Identifikation auf den Systemen und der Zutritt zu den Gebäuden gesperrt.

Zugangskontrolle:

- Der Zugang zu den Systemen der DAUF AG erfolgt mit personalisierten Identifikationen.
- Der Zugang zu den Systemen ist immer mindestens mit einem Passwort oder einem äquivalenten Authentifizierungsmerkmal und der dazugehörenden Benutzerkennungen geschützt.
- Es bestehen Minimalanforderungen an die Passwortkomplexität.
- Bei fehlerhafter Anmeldung wird die Identifikation nach mehreren Fehlversuchen temporär gesperrt. Es besteht ein Prozess zur Rücksetzung gesperrter Identifikationen.

Zugriffkontrolle:

- Die Berechtigungen auf den Systemen sind so strukturiert, dass nur auf die Daten zugegriffen werden kann, die für die Erfüllung der Aufgabe notwendig sind.
- Falls ein Mitarbeiter zusätzliche Rechte benötigt, kann er eine zusätzliche Rolle bestellen. Die Freigabe für diese zusätzliche Rolle erfolgt durch den Rollenbesitzer.
- Für sämtliche Rollen wird regelmässig überprüft, ob die zugeordneten Benutzer diese Rollen noch benötigen.
- Der Datenverkehr zwischen dem Netzwerk des Kunden und der DAUF AG erfolgt nach Möglichkeit verschlüsselt. Die Verschlüsselung kann auf verschiedene Arten erfolgen.
- Das Netzwerk ist durch eine Firewall, durch ein Intrusion Detection System (IDS) sowie durch eine Netzwerksegmentierung geschützt.
- Es sind Virenscanner im Einsatz, welche regelmässig aktualisiert werden.
- Die Server- und Client-Systeme werden regelmässig gepatcht.
- Zugriff auf Daten und Systeme werden protokolliert.

Transportkontrolle:

- Der Zugriff über das Internet auf relevante Daten erfolgt immer über eine verschlüsselte Verbindung.

Speicherkontrolle:

- Die permanenten Speicher in den Rechenzentren verfügen über redundante Stromversorgungen und die notwendigen Systeme, um einen autarken Betrieb für einen definierten Zeitraum zu ermöglichen.
- Zum Schutz vor Rauch- oder Brandschäden verfügen die Rechenzentren über Rauch- und Brandmeldeanlagen.
- Datenträger werden bei Defekt physisch unbrauchbar gemacht oder einem zertifizierten Entsorger übergeben, um einen möglichen Zugriff vollständig auszuschliessen.
- Funktionierende Datenträger werden mit branchenüblichen Löschverfahren so gelöscht, dass eine Rekonstruktion der beinhalteten Daten praktisch unmöglich ist. Ist ein solches Verfahren nicht möglich, werden die Datenträger physisch unbrauchbar gemacht, respektive zerstört.

Eingabekontrolle:

- Eingaben oder Veränderungen in Datenverarbeitungssystemen werden protokolliert.

Verfügbarkeitskontrolle:

- Es werden regelmässige Backups durchgeführt, um den Verlust von Daten im Falle eines Systemproblems zu vermeiden.
- Um die Verfügbarkeit von Daten zu gewährleisten, werden die Speichersysteme so konfiguriert, dass auch mehr als eine Komponente ausfallen kann und die Daten trotzdem noch verfügbar sind.

Trennungsgebot:

- Es wird auf logischer und physischer Ebene sichergestellt, dass die Daten der Kunden nicht gegenseitig einsehbar sind.

Überprüfung, Bewertung und Evaluierung:

- Es werden periodisch Audits durchgeführt.
- Die IT-Sicherheitseinrichtungen werden wiederkehrend einem, von externen Experten durchgeführten IT Security Audit unterzogen.