Auftragsbearbeitungsvertrag

bexio AG

Dieser Auftragsbearbeitungsvertrag konkretisiert die Verpflichtungen betreffend Datenschutz, welche sich aus dem Vertragsverhältnis zwischen der bexio AG (nachfolgend "Provider" oder "Auftragsbearbeiter") und ihren Kundinnen und Kunden (nachfolgend "Auftraggeber" oder "Verantwortlicher") ergeben. Für sämtliche anfallende Datenschutzfragen kann der Auftraggeber den Datenschutzbeauftragen des Providers über datenschutz@bexio.com erreichen.

1. Gegenstand

1.1. Zwischen den Parteien besteht ein Rechtsverhältnis, für dessen Durchführung Personendaten vom Verantwortlichen an den Auftragsbearbeiter übertragen werden ("Hauptvertrag"). Grundlage für das Rechtsverhältnis der Parteien bilden die Allgemeinen Geschäftsbedingungen ("AGB") des Providers. Der vorliegende Auftragsbearbeitungsvertrag wird zwischen den Parteien geschlossen, um bei der Übertragung von Personendaten einen angemessenen Schutz zu gewährleisten.

1.2. Solange in dieser Vereinbarung nicht abweichend bestimmt, sollen alle Begrifflichkeiten dieselbe Bedeutung haben, wie im Schweizer Datenschutzgesetz ("DSG"). Ferner unterstützt diese Vereinbarung die Parteien bei der Einhaltung der Datenschutz-Grundverordnung der EU ("DSGVO"), soweit diesbezüglich geschützte Personendaten von Kunden aus dem EU-Raum betroffen sind.

2. Beschreibung der Datenbearbeitung

2.1. Der Provider bearbeitet Personendaten im Auftrag des Auftraggebers. Gegenstand und Dauer des Vertragsverhältnisses sowie Art und Zweck der Bearbeitungen ergeben sich grundsätzlich aus den AGB sowie dem Anhang A zum Auftragsbearbeitungsvertrag. Die Datenbearbeitungen werden ausserdem in der aktuellen Leistungsbeschreibung auf der Website des Providers sowie in der Datenschutzerklärung ("DSE") konkretisiert.

2.2. Durch Ausfüllen der Anmeldemaske zur Registrierung und Bestellung eines Benutzerkontos ("bexio-Konto") auf der Website des Providers erteilt der Auftraggeber dem Provider die entsprechende Weisung zur Datenbearbeitung. Der Auftraggeber kann seine Weisungen in seinem bexio-Konto oder durch Mitteilung an den Provider ergänzen, ändern oder zurückziehen. Weisungen, die in den AGB nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder durch entsprechende Vornahme im bexio-Konto durch den Auftraggeber nachzuholen.

3. Pflichten des Auftraggebers

3.1. Der Auftraggeber ist im Rahmen des Vertragsverhältnisses für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an den Provider sowie für die Rechtmässigkeit der Datenbearbeitung allein verantwortlich.

3.2. Der Auftraggeber hat sich davon überzeugt, dass die durch den Auftragsbearbeiter eingesetzten, in Anhang B beschriebenen, technischen und organisatorischen Massnahmen ("TOM") ausreichend sind, um für die übertragenen Personendaten einen angemessenen Datenschutz sicherzustellen.

3.3. Der Auftraggeber hat den Provider unverzüglich und vollständig schriftlich oder über das bexio-Konto zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.4. Der Auftraggeber nennt dem Provider den Ansprechpartner für im Rahmen des Vertragsverhältnisses anfallende Datenschutzfragen, sofern dieser von der genannten Ansprechperson abweicht.

3.5. Der Auftraggeber erklärt, dass er die alleinige Verantwortung trägt für die Information der von der Datenbearbeitung betroffenen Personen betreffend der möglichen Datenspeicherung, -nutzung, -bearbeitung und -weitergabe durch den Provider gemäss den Bestimmungen in den AGB, der DSE und diesem Auftragsbearbeitungsvertrag. Sollten einzelne betroffene Personen mit der vorgesehenen Datenbearbeitung nicht einverstanden sein, ist der Auftraggeber verantwortlich die jeweiligen Daten in seinem bexio-Konto entsprechend zu löschen.

3.6. Mit Akzeptierung der AGB sowie dem Auftragsbearbeitungsvertrag erklärt der Auftraggeber **ausdrücklich sein Einverständnis zur Weitergabe seiner Daten an die Muttergesellschaft des Providers** sowie verbundene Gesellschaften. Der Auftraggeber befreit den Provider von jeglichen möglichen Ansprüchen. Die Einholung des Einverständnisses der betroffenen Personen ist Sache des Auftraggebers.

4. Pflichten des Providers

4.1. Allgemein

4.1.1. Der Auftragsbearbeiter sichert in Bezug auf die Bearbeitung der Personendaten zu, dass er

- diese Personendaten in Einklang mit vorliegendem Auftragsbearbeitungsvertrag und ausschliesslich für die Zwecke, die der Verantwortliche verfolgt, bearbeiten wird,
- die Zwecke, die der Verantwortliche verfolgt, sich aus Anhang A, aus dem bexio-Konto oder aus den ausdrücklichen Weisungen des Verantwortlichen ergeben oder durch eine andere Vereinbarung mit dem Verantwortlichen festgelegt werden,
- dem Verantwortlichen diejenigen Informationen zur Verfügung stellen wird, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind,

- bei seinen Arbeitsmitteln, Produkten, Anwendungen oder Dienstleistungen die Grundsätze des Data Privacy by Design und by Default berücksichtigt,

- den Verantwortlichen informieren wird, wenn er diese Vereinbarung nicht mehr einhalten kann oder voraussichtlich nicht mehr einhalten können wird, und

- mit den zuständigen Aufsichtsbehörden im gesetzlich zulässigen Rahmen kooperieren wird.

4.1.2. Weisungsberechtigte Personen des Verantwortlichen werden dem Auftragsbearbeiter zu Beginn der Auftragsbearbeitung schriftlich oder im bexio-Konto mitgeteilt. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Provider unverzüglich schriftlich oder im bexio-Konto der Nachfolger bzw. der Vertreter mitzuteilen. Mündliche Weisungen sind nur bei unmittelbarer schriftlicher Bestätigung des Verantwortlichen verbindlich. E-Mail ist für die Wahrung der Schriftform ausreichend.

4.1.3. Der Provider hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Gesetzesvorschriften. Der Provider ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis ihre Gesetzmässigkeit durch den Verantwortlichen bestätigt oder die Weisung geändert wird.

4.2. Datensicherheit

4.2.1. Der Provider gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so aus, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft technische und organisatorische Massnahmen zum angemessenen Schutz der Personendaten des Auftraggebers, die den jeweiligen gesetzlichen Anforderungen genügen. Der Auftragsbearbeiter hat dabei den Stand der Technik, die Implementierungskosten und die Art, den Umfang und die Zwecke der Bearbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Grund- und Persönlichkeitsrechte betroffener Personen berücksichtigt. Die Massnahmen sind in Anhang B beschrieben und werden periodisch überprüft. Änderungen der Massnahmen sind zulässig, sofern das bisherige Sicherheitsniveau nicht unterschritten wird. Dem Auftraggeber sind diese technischen und organisatorischen Massnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu bearbeitenden Daten ein angemessenes Schutzniveau bieten.

4.2.2. Der Provider wird bei der Durchführung der Arbeiten nur Beschäftigte einsetzen, die zur Vertraulichkeit verpflichtet sind und die zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

4.2.3. Der Provider unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der datenschutzrechtlichen Anfragen und Ansprüche betroffener Personen sowie bei der Einhaltung der datenschutzrechtlichen Pflichten. Der Provider ist gemäss AGB berechtigt, hierfür eine Aufwandsentschädigung zu verlangen.

4.2.4. Sofern dem Provider Verletzung des Schutzes von Personendaten bekannt werden, trifft er die zumutbaren Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen. Ausserdem hält der Provider die geltenden gesetzlichen Bestimmungen betreffend Meldung von Verletzungen des Datenschutzes vollumfänglich ein.

5. Subunternehmer (weitere Auftragsbearbeiter)

5.1. Der Provider kann zur Erfüllung der vertraglichen Leistung Subunternehmer beiziehen. Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen. Die Beauftragung von Subunternehmern als Auftragsbearbeiter durch den Provider ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen des vorliegenden Auftragsbearbeitungsvertrages erfüllen. Der Provider trifft mit den Subunternehmern im erforderlichen Umfang Vereinbarungen, um angemessene Datenschutz- und Informationssicherheitsmassnahmen zu gewährleisten. Subunternehmer, welche keinen Zugriff auf Personendaten haben bzw. keine Bearbeitung von Personendaten als Auftragsbearbeiter vornehmen, sind von diesem Kapitel ausgenommen. Eine Liste der aktuellen Subunternehmer im Sinne eines Auftragsbearbeiters (nachfolgend einfachheitshalber nur "Subunternehmer") ist hier abrufbar:

https://www.bexio.com/de-CH/richtlinien/subunternehmer

5.2. Der Auftraggeber stimmt zu, dass der Provider die auf der Website des Providers genannten Subunternehmer hinzuzieht. Vor Hinzuziehung weiterer Subunternehmer informiert der Provider den Auftraggeber durch Aktualisierung seiner Website. Die Übersicht auf der Website ist jeweils mindestens 14 Tage vor Hinzuziehung zu aktualisieren. Der Auftraggeber wird regelmässig die Übersicht einsehen. Der Auftraggeber kann der Änderung innert 14 Tagen seit Kenntnisnahme aus wichtigem Grund widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Provider ein Sonderkündigungsrecht eingeräumt.

5.3. In der Regel nicht als Unterauftragsbearbeitung gelten Nebenleistungen für den Provider ohne Bezug zu den Daten des Verantwortlichen gemäss Anhang A (z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservices oder die Entsorgung von Datenträgern sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software). Der Provider ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei Nebenleistungen angemessene Kontrollmassnahmen zu ergreifen.

6. Bekanntgabe ins Ausland

6.1. Die Bearbeitung der Daten gemäss Anhang A findet grundsätzlich in der Schweiz oder einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein anderweitiges Drittland darf nur erfolgen, wenn die entsprechenden gesetzlichen Voraussetzungen erfüllt sind.

6.2. Setzt der Auftragsbearbeiter Subunternehmer in Staaten ein, die gemäss Eidgenössischem Datenschutz- und Öffentlichkeitsbeauftragten, Anhang zur VDSG oder EU-Kommission kein angemessenes Datenschutzniveau besitzen, stellt der Auftragsbearbeiter die datenschutzrechtliche Zulässigkeit der Bekanntgabe durch entsprechende, dem jeweiligen Datentransfer angemessene Massnahmen sicher.

7. Rechte der betroffenen Personen

7.1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Provider, wird der Provider die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Provider leitet den Antrag der betroffenen Person innert angemessener Frist an den Auftraggeber weiter. Der Provider kann den Auftraggeber bei datenschutzrechtlichen Ansprüchen einer betroffenen Person im Rahmen seiner Möglichkeiten unterstützen. Der Provider ist in diesem Fall berechtigt, eine Aufwandsentschädigung zu verlangen. Der Provider haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Nachweismöglichkeiten

8.1. Der Provider weist dem Auftraggeber die Einhaltung der in dieser Anlage niedergelegten Pflichten mit geeigneten Mitteln nach. Dies erfolgt durch einen Selbstaudit und/oder ISO-Zertifizierung.

8.2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein (z.B. aufgrund Unterstellung DSGVO), werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Provider darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Massnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Provider stehen, kann der Provider diesen ablehnen und eine neutrale Person vorschlagen. Allfällige mit der Prüfung verbundene Kosten kann der Provider dem Auftraggeber in Rechnung stellen, insbesondere wenn keine Unregelmässigkeiten festgestellt werden konnten.

8.3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt vorliegendes Kapitel entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoss nach dem Strafgesetzbuch strafbewehrt ist.

9. Informationspflichten

9.1. Sollten die Daten des Auftraggebers beim Provider durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat der Provider den Auftraggeber unverzüglich darüber zu informieren. Der Provider wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschliesslich beim Auftraggeber liegen.

10. Dauer und Beendigung

10.1. Der Provider bearbeitet und speichert Personendaten, solange das Vertragsverhältnis zwischen dem Provider und dem Auftraggeber besteht. Der Provider berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Davon ausgenommen sind Daten, welche für die Weiterbearbeitung aufgrund gesetzlicher Vorschriften oder für zwingende interne Zwecke erforderlich sind. Der Provider ist berechtigt, die Durchführung von allfälligen missbräuchlichen Weisungen so lange auszusetzen, bis ihre Gesetzmässigkeit nachgewiesen ist. Die Herausgabe der Daten und die entsprechende Vergütung ist in den AGB geregelt.

11. Haftung

11.1. Die Haftung richtet sich nach den entsprechenden Bestimmungen in den AGB.

12. Sonstiges

12.1. Im Übrigen gelten die Bestimmungen in den AGB und DSE. Bei etwaigen Widersprüchen zwischen dem Auftragsbearbeitungsvertrag und den AGB gehen die Bestimmungen in den AGB vor. Sollten einzelne Teile des Auftragsbearbeitungsvertrag unwirksam sein, so berührt dies die Wirksamkeit der AGB und der übrigen Bestimmungen des Auftragsbearbeitungsvertrages nicht.

12.2. Anhang A und Anhang B sind wesentliche Bestandteile des vorliegenden Auftragsbearbeitungsvertrages.

Letzte Version: September 2023

bexio AG

Alte Jonastrasse 24

8640 Rapperswil

Schweiz

Anhang A Gegenstand, Art und Zweck

Anhang B Technische und organisatorische Massnahmen (TOM)

1. Anhang A – Gegenstand, Art und Zweck

Gegenstand des Auftrags:	Bearbeitung von Personendaten des Auftraggebers im Rahmen seiner Nutzung der Leistungen des Providers als Software as a Service.
Art und Zweck der vorgesehenen Bearbeitung von Daten:	Die vom Auftraggeber bearbeiteten Personendaten werden an den Provider im Rahmen der Software as a Service Leistungen übertragen. Der Provider bearbeitet diese Daten ausschliesslich gemäss den AGB und dem entsprechenden Leistungsbeschrieb auf der Website des Providers (Auftragsverwaltung, Kontaktverwaltung (CRM), Buchhaltung, E-Banking, Lohnbuchhaltung, Lagerverwaltung, Projektverwaltung, etc.).
Art der Personendaten:	Die Datenarten hängen von den durch den Auftraggeber übermittelten Daten ab. Diese sind insbesondere (abhängig vom Auftrag): ● Personenstammdaten (Name, Geburtsdatum, Anschrift, Arbeitgeber) einschliesslich Kontaktdaten (z.B. Telefon, E-Mail) ● Vertragsdaten, einschliesslich Abrechnung und Zahlungsdaten ● Historie der Vertragsdaten
Kategorien betroffener Personen:	Die Kategorien der betroffenen Personen hängen von den durch den Auftraggeber übermittelten Daten ab. Diese sind insbesondere (abhängig vom Auftrag): ● Mitarbeiter (einschliesslich Bewerber und ehemaligen Mitarbeitern) des Auftraggebers ● Kunden des Auftraggebers ● Interessenten des Auftraggebers ● Dienstleister des Auftraggebers ● Kontaktdaten zu Ansprechpartnern
Löschung, Sperrung und Berichtigung von Daten:	Anfragen zur Löschung, Sperrung und Berichtigung sind an den Auftraggeber zu richten; im Übrigen gelten die Regelungen in den AGB, in der DSE und dem vorliegenden Auftragsbearbeitungsvertrag.

2. Anhang B - Technische und organisatorische Massnahmen (TOM)

I. Zutrittskontrolle:

Massnahmen, mit denen Unbefugten der Zutritt zu Datenbearbeitungsanlagen verwehrt wird, mit denen Personendaten bearbeitet oder genutzt werden:

- Alarmsystem
- Automatisierte Zutrittskontrolle
- Fotoelektronische Sensoren / Bewegungsmelder
- Schlüssel-Management (Schlüssel-Herausgabe, etc.)
- Chip-Karten / Transponder Verschlusssystem
- Manuelles Verschlusssystem (auf Schlüsselpersonen beschränkte Nutzung bei Fehler in Zutrittskontrollsystemen)
- Videoüberwachung im Eingangsbereich
- Sichtbares und obligatorisches Badge-Tragen
- Festlegung von Sicherheitsbereichen
- Festlegung zutrittsberechtigter Personen
- Eine separate und dokumentierte Kontrolle zum Zutritt in Rechenzentren und Serverräume nur für besonders befugtes Personal ist implementiert. Der Zutritt durch befugtes Personal wird protokolliert mit Namen und Karten- oder Token-Nummer. Für Rechenzentren existieren separate Zutrittskontrollen.

II. Zugangskontrolle:

Massnahmen, mit denen die Nutzung von Datenbearbeitungssystemen durch Unbefugte verhindert wird:

- Vergabe von Benutzerrechten
- Passwortvergabe
- Authentifizierung mit Benutzername / Passwort / MFA
- Automatische Zugangssperre
- Manuelle Zugangssperre
- Protokollierung des Zugangs
- Verwendung von Hardware Firewalls
- Verwendung von User Profilen
- Zusätzliche Massnahmen: web-application firewalls, regelmässige vulnerability scans, regelmässiges penetration testing, patch management, Minimalvoraussetzungen für Passwortkomplexität und erzwungener Passwortwechsel, Verwendung von Virenscannern.
- Zuordnung von User Profilen zu IT Systemen
- Verwendung von VPN Technologie
- Verschlüsselung mobiler Speichermedien
- Verwendung eines Mobile-Device-Managements (zum Beispiel: remote locking and wiping von Smartphones)
- Hardwareverschlüsselung für Notebooks

III. Zugriffskontrolle:

Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenbearbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen

können, und dass Personendaten bei der Bearbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

- Schaffung eines Autorisierungskonzepts (Identity Access Management)
- Anzahl Administratoren aufs “absolute Minimum” reduziert
- Vergabe minimaler Berechtigungen
- Umsetzen von Zugriffsbeschränkungen
- Sichere Medienbereinigung vor der Wiederverwendung
- Hardwareverschlüsselung (Backup-Tapes, Notebooks)
- Rechteverwaltung durch Systemadministratoren
- Passwort-Richtlinie mit Vorgaben zur Passwortlänge, Passwort Change-Management
- Sichere Aufbewahrung von Datenträgern

IV. Bekanntgabekontrolle

Massnahmen, die gewährleisten, dass Personendaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Personendaten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Schaffung einer Standleitung oder einer VPN-Verbindung
- Verschlüsselung (Backup für off-site Speicherung)
- TLS Verschlüsselung für alle Kommunikation (Web-Client, APIs, mobile Apps)
- Sicherung der Übertragung im Backend
- Sicherung der Übertragung zu externen Systemen
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
- Maschine-Maschine Authentisierung
- Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

V. Eingabekontrolle

Massnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem Personendaten in Datenbearbeitungssystemen eingegeben, verändert oder entfernt werden können:

- Rechtevergabe für Eingabe, Modifikation und Löschung von Daten basierend auf einem Authorisierungskonzept
- Automatische Dokumentation der Eingabeberechtigungen
- Protokollierung der Eingaben

VI. Verfügbarkeitskontrolle

Massnahmen, die gewährleisten, dass Personendaten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (UPS)
- Vorrichtungen, um Temperatur und Feuchtigkeit in Serverräumen zu überwachen
- Feuer- und Rauchmeldesysteme
- Alarmierung, wenn unbefugter Zutritt zu Serverräumen erfolgt
- Schaffung von Backup- & Wiederherstellungskonzepten
- Erstellen von Datenbackups
- Testen der Datenwiederherstellung

- Sichere off-site Speicher von Datenbackups
- Klimaanlagen in Serverräumen
- Löschanlagen in Serverräumen
- Notfallplan
- Aufbewahrung der Backups
- Prüfung der Notfalleinrichtungen

VII. Gebot der Trennung

Massnahmen, die gewährleisten, dass Personendaten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt bearbeitet werden:

- Schaffung eines Autorisierungskonzepts
- Bewilligte und dokumentierte Datenbankrechte
- Logical Client Separation/logische Mandantentrennung (auf Stufe Software)
- Trennung von produktiven und Testsystemen
- Sparsamkeit bei der Datenerhebung