swiss direct marketing
creating response

Vertrag zur Auftragsbearbeitung (ABV) nach Schweizer Datenschutzgesetz (DSG)

Präambel

Swiss Direct Marketing AG in Brugg/AG (fortan: SDM) erbringt Dienstleistungen im Bereich Marketing, insbesondere Konzeption, Gestaltung, Herstellung, Verpackung und Versand von gedruckten oder digitalen Direkt-Marketing-Mitteln und weiteren Waren sowie Handel mit Waren aller Art.

Die SDM steht für die Entwicklung und Umsetzung von personalisierten, medienübergreifenden Direct Marketing Kampagnen und übernimmt von der Konzeption über das Datenmanagement bis hin zur Realisation alle für den Kampagnenerfolg notwendigen Leistungen. Die SDM bearbeitet Daten im Auftrag ihrer Kunden. Die Daten werden nicht durch die SDM selber erhoben, sondern von den Kunden der SDM zur Verfügung gestellt. Die SDM verwendet die Daten gemäss Auftrag.

Für die Realisierung von Kampagnen gemäss separat abgeschlossenen Verträgen oder Aufträgen wird die SDM von Auftraggebern für die Bearbeitung von Daten beigezogen. Der Beizug wird ergänzend zu den anderen zwischen den Parteien geltenden Verträgen oder Aufträgen im vorliegenden Vertrag zur Auftragsbearbeitung (ABV) geregelt.

Für den vorliegenden Vertrag sowie die anderen gültigen Verträge oder Aufträge zwischen den Parteien gilt das jeweils aktuell anwendbare Datenschutzrecht. Die im vorliegenden ABV referenzierten gesetzlichen Grundlagen betreffen das totalrevidierte Datenschutzrecht der Schweiz (in Kraft ab 1. September 2023).

1. Zweck des Dokuments, Begriffe

Die vorliegende Vereinbarung konkretisiert die Verpflichtungen der SDM (nachstehend: Auftragnehmerin) und des Auftraggebers (= Kunde), (gemeinsam: die Parteien) in Bezug auf die Vorgaben aus den anwendbaren Schweizer Datenschutzgesetzen.

Dieser ABV kommt nur zusammen mit einem schriftlichen Vertrag oder Auftrag zur Anwendung. Konkretisierungen zu einzelnen Bestimmungen dieses ABV können im schriftlichen Vertrag oder Auftrag sowie deren Anhängen festgehalten werden.

Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der anwendbaren gesetzlichen Bestimmungen für die Rechtmässigkeit der Datenbearbeitung an sich inklusive der Zulässigkeit der Auftragsbearbeitung durch die Auftragnehmerin verantwortlich. Der Auftraggeber garantiert, dass die Daten rechtmässig und unter Einhaltung aller anwendbaren gesetzlichen Bestimmungen erhoben wurden, dass die Überlassung der Daten an die Auftragnehmerin zur Bearbeitung und alle an die Auftragnehmerin im Hinblick auf die Bearbeitung der Daten erteilten Weisungen rechtmässig sind und keine Rechte Dritter verletzen. Der Auftraggeber ist insbesondere dafür verantwortlich, allfällig erforderliche Einwilligungen der betroffenen Personen und Institutionen einzuholen.

2. Gegenstand, Dauer und Ort

2.1 Gegenstand des Auftrags

Der Gegenstand der Datenbearbeitung, ihre Art und ihr Zweck sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich in erster Linie aus dem Vertrag oder der Auftragsbestätigung und allfälligen Anhängen.

Die Auftragnehmerin darf die Daten in keinem Fall zu eigenen Zwecken bearbeiten, wie etwa zu Marketingzwecken, für eigene Geschäftstätigkeit oder für Bonitätsauskünfte etc.

2.2 Dauer

Der Auftrag beginnt mit Unterzeichnung des Vertrags oder einer Auftragsbestätigung und endet mit einer Kündigung bzw. dem Vertragsablauf.

Sollte die Zusammenarbeit auf verschiedenen Einzelverträgen oder Aufträgen basieren, so bleibt der vorliegende ABV bis zur Beendigung der Zusammenarbeit hinsichtlich des letzten Einzelvertrags zwischen den Parteien gültig.

2.3 Ort der Datenbearbeitung

Die Bearbeitung der Daten im Auftrag des Auftraggebers findet auf dem Gebiet der Schweiz statt. Eine Bearbeitung in einem Staat ausserhalb der Schweiz ist nur zulässig, wenn sichergestellt das durch das DSG gewährleistete Schutzniveau nicht unterlaufen wird und eine vorherige ausdrücklichen schriftliche Zustimmung des Auftraggebers vorliegt. Die grundlegenden Voraussetzungen für die Rechtmässigkeit der Bearbeitung bleiben unberührt.

Sofern Bearbeitungen in einem Land ohne angemessenes Datenschutzniveau gemäss der jeweiligen Definition des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)/des Bundesrates durchgeführt werden sollen, bedarf dies neben der vorherigen schriftlichen Zustimmung durch den Verantwortlichen zusätzlicher Datenschutzgarantien, welche schriftlich zu vereinbaren sind. Geeignet sind hierzu z.B. Standarddatenschutzklauseln, welche dem EDÖB vorgängig mitzuteilen sind.

3. Weisungsgebundene Bearbeitung

Die Auftragnehmerin verpflichtet sich, die Personendaten ausschliesslich für die Erfüllung ihrer vertraglichen Pflichten gemäss den Bestimmungen des Vertrags und allfälliger Anhänge sowie im Auftrag und auf dokumentierte Weisungen des Auftraggebers zu bearbeiten und sicherzustellen, dass die definierte Datenbearbeitung datenschutzkonform durchgeführt wird.

Weisungen werden vom Auftraggeber grundsätzlich in Textform (z.B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese entsprechend in Textform (z.B. per E-Mail) bestätigt.

Die Auftragnehmerin wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach ihrer Ansicht gegen das Schweizer Datenschutzgesetz oder eine andere Vorschrift über den Datenschutz verstösst.

4. Sicherheit der Datenbearbeitung / Organisatorische und technische Massnahmen

Die Auftragnehmerin ergreift alle erforderlichen technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Bearbeitung nach der anwendbaren Gesetzgebung. Die durch die Auftragnehmerin zu treffenden Massnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei ist insbesondere zu beachten, dass der Auftraggeber unter Umständen besonders schützenswerte Daten bearbeitet.

Technische und organisatorische Massnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch die Auftragnehmerin fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in Anhang 1 festgelegten technischen und organisatorischen Massnahmen darf nicht unterschritten werden.

Die Auftragnehmerin verpflichtet sich, Änderungen der technischen und organisatorischen Massnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der in Anhang 1 genannten Massnahmen schriftlich zu dokumentieren. Dies kann auch in einem elektronischen Format erfolgen und dem Auftraggeber zur Kenntnis gebracht werden.

Die Auftragnehmerin stellt mittels regelmässiger Schulungs- und Sensibilisierungsmassnahmen sicher, dass die von ihr zur Datenbearbeitung eingesetzten Personen die relevanten datenschutzrechtlichen Bestimmungen kennen und einhalten.

5. Inanspruchnahme weiterer (Unter-)-Auftragnehmer

Die Auftragnehmerin ist befugt, zur Bearbeitung der Daten Unterauftragnehmer beizuziehen, soweit sämtliche vertraglichen Bestimmungen, welche zwischen Auftraggeber und Auftragnehmer gelten, auch in Bezug auf den Unterauftragnehmer eingehalten werden.

Die Auftragnehmerin wählt ihre Unterauftragnehmer sorgfältig aus und stellt dem Auftraggeber die entsprechende Dokumentation auf Anfrage zur Verfügung.

In stichhaltig begründeten Fällen hat der Auftraggeber die Möglichkeit, innert 30 Tagen nach Erhalt der Dokumentation, einen Unterauftragnehmer abzulehnen, wenn die Bearbeitung durch den bestimmten Unterauftragnehmer dem Auftraggeber nicht zugemutet werden kann.

Die Auftragnehmerin ist verantwortlich dafür, die Beziehungen schriftlich so zu regeln, dass für Unterauftragnehmer dieselben Bedingungen (Anweisungen, Verpflichtungen, Sicherheitsmassnahmen, etc.) und dieselben formellen Anforderungen hinsichtlich einer angemessenen Bearbeitung der betroffenen personenbezogenen Daten gelten wie für die Auftragnehmerin selbst.

Die Regelungen gemäss Ziff. 9 nachstehend gelten auch für Unterauftragnehmer.

Die Unterauftragnehmer werden über die Dauer des Unterauftragnehmer-Verhältnisses hinaus zur Verschwiegenheit und zum Geheimnisschutz verpflichtet. Ebenso ist die Auftragnehmerin dafür besorgt, dass der Unterauftragnehmer die Verschwiegenheit und Geheimnispflicht beigezogenen Hilfspersonen (u.a. Mitarbeitende) vertraglich.

6. Mitwirkungs- und Unterstützungspflichten

6.1 Mitwirkungspflichten der Auftragnehmerin

Die Auftragnehmerin unterstützt den Auftraggeber angesichts der Art der Bearbeitung mit geeigneten technischen und organisatorischen Massnahmen dabei, seiner Pflicht zur Wahrung der Betroffenenrechte nachzukommen (Recht auf Auskunft; Berichtigungsrecht; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelentscheidungen etc.).

6.2 Unterstützung zur Pflichterfüllung des Auftraggebers

Die Auftragnehmerin unterstützt den Auftraggeber unter Berücksichtigung der Art der Bearbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung weiterer gesetzlichen Pflichten (Gewährleistung der Sicherheit der Bearbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung).

7. Löschung und Rückgabe personenbezogener Daten

Nach Beendigung des Auftrags zur Datenbearbeitung ist die Auftragnehmerin verpflichtet, sämtliche personenbezogenen Daten dem Auftraggeber in einem gängigen und für den Auftraggeber lesbaren Format zurückzugeben oder in dessen Auftrag sowie gemäss dessen Weisung datenschutzkonform zu vernichten/zu löschen, soweit dem nicht gesetzliche oder anderweitige Aufbewahrungspflichten entgegenstehen.

Klarstellend bedeutet dies, dass die Personendaten, die der Auftragnehmer für eine einzelne Kampagne erhält, innerhalb von 4 Wochen nach Abschluss dieses Auftrags die entsprechenden Daten löscht und ein entsprechendes Löschprotokoll führt. Auf Verlangen wird das Löschprotokoll dem Auftraggeber zugstellt.

8. Pflichtennachweis und Unterstützung bei Überprüfungen

Die Auftragnehmerin stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 7 DSG festgelegten Pflichten zur Verfügung.

Der Auftraggeber hat das Recht, bei der Auftragsnehmerin die Einhaltung der gesetzlichen und vertraglichen Pflichten im Zusammenhang mit der Bearbeitung von Daten gestützt auf diese Vereinbarung und die Regelungen aus dem Vertrag oder Auftrag sowie dessen Anhängen durch einen Audit vor Ort zu prüfen. Der Auftraggeber ist verpflichtet, bei einem Audit jeweils angemessen mitzuwirken. Die Parteien einigen sich im Vorfeld über Zeitpunkt, Dauer und Gegenstand der Prüfungen und über anwendbare Sicherheits- und Vertraulichkeitsbestimmungen.

Der Auftraggeber hat das Recht, auf eigene Kosten eine Kontrolle gemäss dieser Ziffer durch eine externe, fachkundige und zur Vertraulichkeit verpflichtete Stelle (nachfolgend «Dritter») durchführen zu lassen. Sie darf keinen Konkurrenten oder Wettbewerber der Auftragnehmerin mit der Kontrolle beauftragen. Das Audit wird zu den üblichen Geschäftszeiten möglichst ohne Störung des Betriebsablaufs nach angemessener Voranmeldung von mindestens 30 Tagen im Voraus durchgeführt, sofern nicht zwingende Bestimmungen des anwendbaren Datenschutzrechts oder eine Datenschutzbehörde kürzere Fristen vorschreiben. Das Audit des Auftraggebers ist auf maximal einen Arbeitstag pro Kalenderjahr beschränkt. Jede Partei

trägt die bei ihr anfallenden Kosten und Ausgaben im Zusammenhang mit einer Kontrolle gemäss dieser Ziffer selber. Bei einem über einen Arbeitstag hinausgehenden Aufwand kann die Auftragnehmerin für die Unterstützung bei der Durchführung eines vom Auftraggeber veranlassten Audits von jenem eine Vergütung verlangen.

Stellt der Auftraggeber bzw. der Dritte im Rahmen dieser Kontrollen einen Verstoss gegen die Bedingungen dieses ADV fest, teilt er die Mängel der Auftragnehmerin umgehend mit. Der Auftraggeber und die Auftragnehmerin werden sich auf eine angemessene Weise über die notwendigen Korrekturmassnahmen einigen. Die Auftragnehmerin verpflichtet sich, die zwischen den Parteien vereinbarten notwendigen Korrekturmassnahmen innert vereinbarter Frist durchzuführen.

9. Vertraulichkeit und Geheimnisschutz

Grundsätzlich gelten sämtliche anvertrauten Informationen, wie auch die Information über bestehende, zukünftige oder abgelaufene Vertragsverhältnisse oder Aufträge als vertraulich.

Die Parteien sichern sich gegenseitig zu, erhaltene vertrauliche Informationen:

a) Geheim zu halten;

b) Nur für den Vertragszweck zu nutzen;

c) Nicht sonst weiter zu verwerten.

Der Auftragnehmer verpflichtet sich insbesondere absolutes Stillschweigen zu bewahren über:

a) Tätigkeiten und Inhalte im Rahmen der Vertrags- oder Auftragsverhältnisse

b) Dem Datenschutz unterliegende Personendaten

c) Den Informationen über die Kundenbeziehungen

Die Schweigepflicht dauert uneingeschränkt über das Vertragsverhältnis hinaus.

Ohne ausdrückliche Einwilligung dürfen keinerlei Daten, Informationen, Geschäftsakten, Speichermedien o.ä., weder im Original noch in Kopie, ganz oder auszugsweise entfernt, mitgenommen oder in den persönlichen Besitz überführt werden oder unbefugten Dritten in irgendwelcher Art und Weise zugänglich oder bekannt gemacht werden.

Um den Vertragszweck zu erreichen werden Mitarbeiter oder Hilfspersonen von der Auftragnehmerin mit Vertrag oder mit einer Geheimhaltungserklärung zum Geheimnis verpflichtet. Diese Pflicht muss mindestens so streng formuliert sein, wie die in diesem Vertrag auferlegte Geheimhaltungspflicht.

Ein Geheimnis darf nur soweit offengelegt werden, als dies aufgrund einer gesetzlichen Pflicht notwendig wird. Sollte ein derartiger Fall eintreffen, verpflichten sich die Parteien, die jeweils andere Partei unmittelbar schriftlich davon in Kenntnis zu setzen, sodass die betroffene Partei allenfalls notwendige Massnahmen einleiten oder den Rechtsweg beschreiten kann.

Die Verletzung der Schweigepflicht kann privatrechtliche und strafrechtliche Konsequenzen nach sich ziehen.

Die Verpflichtung zum Geheimnis entfällt, wenn:

a) Es sich im Zeitpunkt der Offenlegung um eine öffentlich bekannte Tatsache handelt.

b) Die Information öffentlich wurde, ohne dass eine Veröffentlichung durch die Auftragnehmerin unberechtigten Dritten gegenüber gemacht wurde.

c) Die Auftragnehmerin rechtmässig zur Information gelangt ist.

d) Die Information durch eigene, unabhängige Entwicklung erlangt wurde.

e) Eine gesetzliche Pflicht zur Offenlegung besteht (bspw. Auskunftsrecht)

10. Kontakt/Datenschutzberater

Kontaktstelle beim Auftraggeber für die Auftragsnehmerin für Belange gemäss vorliegendem ABV ist:

Swiss Direct Marketing AG, Wildischachen 18, 5200 Brugg

Tel. 056 462 82 32, privacy@myelco.ch

11. Schlussbestimmungen

Sollte die auftragsgemässe Erfüllung des Auftragsgegenstandes gemäss Ziff. 1 dieser Vereinbarung bei der Auftragnehmerin durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder ein Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, informiert die Auftragnehmerin den Auftraggeber unverzüglich. Die Auftragnehmerin wird alle in diesem Zusammenhang Beteiligten unverzüglich darüber informieren, dass die Verfügungsbefugnisse an den Daten ausschliesslich beim Auftraggeber liegen.

Bei etwaigen Widersprüchen zwischen diesem Vertrag und zuvor geschlossenen vertraglichen Regelungen gehen die Regelungen dieses Vertrags den zuvor geschlossenen vertraglichen Regelungen vor.

Sollten einzelne Teile dieses Auftrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht. Jede Veränderung dieser Vereinbarung einschliesslich ihrer Kündigung und dieser Klausel bedarf der Schriftform, was auch in einem elektronischen Format erfolgen kann.

Die vorliegende Vereinbarung gilt ab 1. September 2023.

Anhang 1

Technische und organisatorische Massnahmen gemäss Art. 7 DSG und Art. 1 ff. DSV

Unter Berücksichtigung des

• Stands der Technik,

• der Implementierungskosten und

• der Art, des Umfangs, der Umstände und

• der Zwecke der Bearbeitung sowie

• der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

trifft die Auftragnehmerin geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Bearbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmässig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise bearbeitet wurden.

Massnahmen die geeignet sind, Unbefugten den Zutritt zu den Datenbearbeitungsanlagen, mit denen personenbezogene Daten bearbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle).

Es existieren folgende Massnahmen zur Zutrittskontrolle:

- Aktive Überwachung, Sicherung der Servertüren, Sicherheitstüren
- Schliesssystem mit Codesperre (Gebäude ja, Abteilungen, nein, ausser Serverraum))
- Manuelles Schliesssystem (Ja)
- Sicherheitstüren und -schlösser
- Schlüsselregelung (Schlüsselausgabe, Schliessplan etc.)

Massnahmen, die verhindern, dass Datenbearbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle).

Es existieren folgende Massnahmen zur Zugangskontrolle:

- Erstellen von Benutzerprofilen
- Regelmässige Überprüfung der Benutzerkonten
- Passwortvergabe

- Authentifikation mit Benutzername / Passwort
- Einsatz von VPN-Technologie
- Sicherheitsschlösser insb. auch für Entsorgungsbehltnissen von Fehldrucken
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verschlüsselung von Smartphone-Inhalten
- Keine externen mobilen Datenträger und Verschlüsselung der Transfer Server
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenbearbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Bearbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Es existieren folgende Massnahmen zur Zugriffskontrolle:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Profile/Rollen klären
- Funktions- und Mandantentrennung
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemässe Vernichtung von Datenträgern (DIN 66399)
- Massnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. Kopierschutz, Sperrung von USB-Posts, «Data Loss Prevention (DLP)-System»)
- Löschkonzept
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

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 (Weitergabekontrolle).

Es existieren folgende Massnahmen zur Weitergabekontrolle:

- Einrichtungen von VPN-Tunneln
- Protokollierung von Datenübertragungen oder Datentransport
- Protokollierung von lesenden Zugriffen
- Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- Einsatz einer Zwei-Faktor Authentifizierung
- Weitergabe von Daten in verschlüsselter Form (verschlüsselter Transfer-Server)
- Verschlüsselung von Datenträgern in Laptops
- Physischen Datentransporte nach Aussen werden unterlassen
- Verpackungs- und Versandvorschriften
- Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)

Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenbearbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Es existieren folgende Massnahmen zur Eingabekontrolle:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)

Es existieren folgende Massnahmen zur Verfügbarkeitskontrolle:

- Unterbrechungsfreie Stromversorgung (USV)
- Abgesicherter Zutritt zum Server
- Klimaanlage in Serverräumen
- Brandmelder mit Alarmauslösung
- Schutzsteckdosenleisten in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- Virenschutz
- Notfallplan und Notfallmanagement
- Verfügbarkeit von Fachpersonal durch Know-how-Verteilung und Vertretungsregelungen

- Verteilung von IT-Diensten über mehrere Systeme
- Monitoring von IT-Systemen
- Netzwerkplan

Massnahmen zur Sicherstellung der Belastbarkeit

Es existieren folgende Massnahmen zur Sicherstellung der Belastbarkeit:

- Notfallplan für Maschinenausfall
- Redundante Stromversorgung
- Austeichende Kapazität von IT-Systemen und Anlagen
- Verteilung von IT-Diensten über mehrere Systeme
- Redundanten Systeme/Anlagen

Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen

- Interne Audits zur Informationssicherheit und Datenschutz
- Change Management
- Penetrationstests

Weisungskontrolle/Auftragskontrolle

Es werden folgende Massnahmen zur Weisungskontrolle/Auftragskontrolle durchgeführt:

- Vertrag zur Auftragsbearbeitung mit Regelungen zu den Rechten und Pflichten der Auftragsnehmerin und des Auftraggebers
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter bei der Auftragnehmerin
- Verpflichtung der Mitarbeiter zur Vertraulichkeit
- Benennung eines Datenschutzbeauftragten gemäss Art. 10 DSG
- Datenschutzmanager/-koordinator
- Führen eines Verzeichnisses von Bearbeitungstätigkeiten gemäss Art. 12 DSG
- Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten
- Richtlinien/Vorgaben zur Gewährleistung technisch-organisatorischer Massnahmen zur Sicherheit der Bearbeitung
- Prozess zur Weiterleitung von Betroffenenanfragen