Auftragsbearbeitungsvertrag

gem. Art. 9 revDSG (Auftragnehmer)

Kundennummer: 1234
Datum: 01.01.2024
Version: 1.0

zwischen

Muster AG
Musterstrasse 2
vertreten durch Herr Felix Muster

(Nachfolgend Kunde genannt)

Telefon:	061 123 45 67
E-Mail:	f.muster@muster.ch

und

Computer Trend IT-Solution GmbH
Steinengraben 55, 4051 Basel
vertreten durch Herrn Markus Meyer, Co-Geschäftsführer

(Nachfolgend Computer Trend genannt)

Telefon:	+41 61 281 44 81
E-Mail	info@computer-trend.ch

1. Begriffsbestimmungen

1.1 «Personendaten» sind alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.

1.2 «Bearbeiten» meint jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

1.3 «Verantwortlicher» ist eine private Person oder ein Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung von Personendaten entscheidet.

1.4 «Auftragsbearbeiter» ist eine private Person oder ein Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

2. Inhalt der Vereinbarung

2.1 Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, die sich aus dem bestehenden Vertragsverhältnis und den jeweils erteilten Einzelaufträgen und den darin festgelegten Pflichten ergeben. Sie findet Anwendung auf alle Tätigkeiten, die hiermit in Zusammenhang stehen und bei denen Mitarbeiter*innen des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit Personendaten des Auftraggebers in Berührung kommen können.

2.2 In dieser Vereinbarung werden Gegenstand und Dauer des Bearbeitens (Ziffer 3), Art und Zweck des Bearbeitens (Ziffer 4), die Art der Personendaten (Ziffer 5), die Kategorien betroffener Personen (Ziffer 6) und die Pflichten und Rechte der Vertragspartner (Ziffer 7 bis 17) beschrieben.

3. Gegenstand und Dauer der Bearbeitung

3.1 Der Gegenstand der Bearbeitung ergibt sich aus der Anlage zu dieser Vereinbarung.

3.2 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des bestehenden Vertragsverhältnisses und der erteilten Einzelaufträge und tritt mit Unterzeichnung durch beide Vertragspartner in Kraft.

3.3 Die Bearbeitung der Personendaten findet ausschliesslich im Gebiet der Schweizerischen Eidgenossenschaft statt. Jede Verlagerung ins Ausland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 13 und 14 revDSG erfüllt sind.

4. Art und Zweck der Bearbeitung

Art und Zweck des Bearbeitens von Personendaten durch den Auftragnehmer ergeben sich aus der Anlage zu dieser Vereinbarung.

5. Kategorien von Personendaten

Die Art der bearbeiteten Personendaten ergibt sich aus dem bestehenden Vertragsverhältnis und aus dem erteilten Einzelauftrag sowie der Anlage zu dieser Vereinbarung.

6. Kategorien betroffener Personen

Der Kreis der durch den Umgang mit ihren Personendaten im Rahmen dieser Vereinbarung Betroffenen umfasst die in der Anlage genannten Personengruppen.

7. Dokumentierte Weisung

7.1 Der Auftragnehmer darf Daten nur im Rahmen des Auftrags, d.h. im Rahmen der sich aus dem bestehenden Vertragsverhältnis und den erteilten Einzelaufträgen ergebenden Bestimmungen und Weisungen des Auftraggebers bearbeiten.

7.2 Der Auftraggeber ist als Verantwortlicher im Sinne von Art. 5 lit. j revDSG im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmässigkeit der Datenbearbeitung verantwortlich. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit und nach Beendigung dieser Vereinbarung Weisungen an den Auftragnehmer erteilen.

7.3 Jede Weisung des Auftraggebers bedarf der Schrift- oder Textform (z.B. Brief, Fax, E-Mail, SMS, Chatnachricht) und muss nachvollziehbar dokumentiert werden. Es muss stets nachvollzogen werden können, wann von wem eine Weisung an den Auftragnehmer erteilt wurde. Der Auftragnehmer hat nur Weisungen in Schrift- oder Textform zu befolgen.

7.4 Der Auftragnehmer informiert den Auftraggeber so rasch als möglich, falls er der Auffassung ist, dass eine Weisung gegen das revDSG oder gegen andere Datenschutzbestimmungen der Schweizerischen Eidgenossenschaft verstösst.

8. Vertraulichkeit

8.1 Der Auftragnehmer gewährleistet und versichert, dass sich die zur Bearbeitung der Personendaten befugten Personen zur Vertraulichkeit und Geheimhaltung in Bezug auf dem Geheimnisschutz unterliegende Daten verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

8.2 Der Auftragnehmer erbringt auf Anfrage den Nachweis über die Verpflichtung auf Vertraulichkeit und Geheimhaltung.

9. Technische und organisatorische Massnahmen des Auftragnehmers

9.1 Der Verantwortliche arbeitet nur mit Auftragsbearbeitern zusammen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen so durchgeführt werden, dass die Bearbeitung im Einklang mit den Anforderungen des revDSG sowie der DSV erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

9.2 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und des Zwecks der Bearbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit hat der Auftragnehmer geeignete technische und organisatorische Massnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Massnahmen schliessen unter anderem gegebenenfalls Folgendes ein:

a) die bearbeiteten Daten sind nur Berechtigten zugänglich (Vertraulichkeit);
b) die bearbeiteten Daten sind nur verfügbar, wenn sie benötigt werden (Verfügbarkeit);
c) die bearbeiteten Daten können nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
d) die bearbeiteten Daten werden nachvollziehbar bearbeitet (Nachvollziehbarkeit).

9.3 Bei der Beurteilung einer angemessenen Datensicherheit hat der Auftragnehmer die Risiken berücksichtigt, die mit der Bearbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmässig, oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu Personendaten, die übermittelt, gespeichert oder auf andere Weise bearbeitet wurden – verbunden sind.

9.4 Der Auftragnehmer unternimmt Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu Personendaten haben, diese nur auf Anweisung des Verantwortlichen bearbeiten, es sei denn, sie sind nach dem Recht der Schweizerischen Eidgenossenschaft zur Bearbeitung verpflichtet.

9.5 Zur Gewährleistung der Sicherheit und Vertraulichkeit der Daten hat der Auftragnehmer geeignete technische und organisatorische Massnahmen getroffen. Ergänzend hierzu gilt die Anlage „Beschreibung der technischen und organisatorischen Massnahmen“.

10. Einschaltung von weiteren Auftragsbearbeitern

10.1 Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zur Einschaltung weiterer Auftragsbearbeiter im Sinne des Art. 9 revDSG sowie Art. 7 DSV.

10.2 Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Dritter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen begründeten Widerspruch im Laufe von 14 Tagen zu erheben.

10.3 Erteilt der Auftragnehmer Aufträge an weitere Auftragsbearbeiter, so obliegt es dem Auftragnehmer, seine Pflichten aus dieser Vereinbarung dem weiteren Auftragsbearbeiter zu übertragen. Dies gilt insbesondere für die zwischen den Vertragspartnern festgelegten Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit.

11. Rechte der Betroffenen

11.1 Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Bearbeitung von Personendaten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen.

11.2 Der Auftragnehmer trifft insbesondere geeignete technische und organisatorische Massnahmen, um dem Auftraggeber die Erfüllung seiner Pflichten gegenüber den Betroffenen zu ermöglichen.

12. Unterstützung des Auftraggebers

12.1 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Bearbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 8 revDSG sowie in Art. 3 DSV genannten Pflichten zur Datensicherheit sowie zu etwa bestehenden Melde- und Benachrichtigungspflichten, durchzuführenden Datenschutz-Folgenabschätzungen und notwendigen vorgängigen Konsultationen des EDÖB.

12.2 Der Auftragnehmer stellt ein angemessenes Schutzniveau durch technische und organisatorische Massnahmen sicher, welche die Umstände und Zwecke der Bearbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

12.3 Der Auftragnehmer ist verpflichtet, eine Verletzung der Datensicherheit so rasch als möglich an den Auftraggeber zu melden. Der Auftragnehmer unterstützt den Auftraggeber bei dessen Meldeverpflichtung aus Art. 24 revDSG und stellt ihm die etwa benötigten Informationen so rasch als möglich zur Verfügung.

12.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen aus Art. 24 revDSG und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen so rasch als möglich zur Verfügung.

12.5 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwaiger durchzuführender Datenschutz-Folgenabschätzungen gem. Art. 22 revDSG.

12.6 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen etwa notwendiger vorgängiger Konsultationen des EDÖB.

13. Vergütungsregelungen

13.1 Der Auftragnehmer darf dem Auftraggeber Aufwendungen in Rechnung stellen, die ihm durch seine Inanspruchnahme auf Grundlage dieses Vertrags und Erfüllung seiner Pflichten aus diesem Vertrag entstanden sind. Dies gilt nicht, wenn der Auftragnehmer aufgrund der zugrundeliegenden schuldrechtlichen Vereinbarung oder aufgrund einer Pflichtverletzung vertraglich oder gesetzlich verpflichtet ist.

13.2 Der Aufwand ist in Höhe der zwischen den Vertragspartnern vereinbarten Stundensätze zu vergüten. Sind keine Stundensätze vereinbart, kann der Auftragnehmer eine angemessene Vergütung verlangen.

14. Abschluss der Erbringung der Bearbeitungsleistungen

14.1 Nach Beendigung des bestehenden Vertragsverhältnisses und des jeweiligen Einzelauftrags hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Bearbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auf Verlangen auszuhändigen.

14.2 Die Datenträger des Auftragnehmers sind danach auf Verlangen physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist – auf Verlangen des Auftraggebers – in geeigneter Weise zu dokumentieren.

15. Kontrollrechte des Auftraggebers

15.1 Der Auftraggeber hat das Recht, sich vor der Aufnahme der Datenbearbeitung und sodann regelmässig von den technischen und organisatorischen Massnahmen des Auftragnehmers zu überzeugen. Hierfür kann er insbesondere Selbstauskünfte des Auftragnehmers einholen und sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich überzeugen oder einen Dritten hiermit beauftragen.

15.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist insbesondere verpflichtet, die Umsetzung von angemessenen technischen und organisatorischen Massnahmen nachzuweisen. Der Nachweis über solche Massnahmen, die nicht nur den konkreten Einzelauftrag betreffen, kann erfolgen durch:

a) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 13 revDSG und der Verordnung über Datenschutzzertifizierungen (VDSZ);

b) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzberaterinnen und -berater, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

c) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach IKT-Grundschutz oder ISO/IEC 27001).

16. Berichtigung, Einschränkung und Löschung von Daten

16.1 Der Auftragnehmer darf die Daten, die im Auftrag bearbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, einschränken oder löschen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen so rasch als möglich an den Auftraggeber weiterleiten.

16.2 Falls vereinbart, sind das Vorhandensein eines datenschutzkonformen Löschkonzepts, das Recht auf Datenherausgabe und -übertragung sowie die Umsetzung der Rechte auf Berichtigung und Löschung vom Auftragnehmer sicherzustellen.

17. Dokumentationspflichten des Auftragnehmers

17.1 Der Auftragnehmer führt ein Verzeichnis zu allen Kategorien von im Auftrag für den Auftraggeber durchgeführten Tätigkeiten der Bearbeitung. Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

17.2 Der Auftraggeber oder der Auftragnehmer sowie gegebenenfalls der Vertreter des Auftraggebers oder des Auftragnehmers stellen dem EDÖB das Verzeichnis auf Anfrage zur Verfügung.

18. Informationspflichten, Schriftformklausel, Rechtswahl

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

18.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschliesslich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

18.3 Es gilt schweizerisches Recht. Gerichtsstand ist der Sitz des Auftragnehmers.

19. Vertragsunterzeichnung

19.1 Mit Ihrer Unterschrift akzeptieren Sie den Auftragsverarbeitungsvertrag mit der Computer Trend IT-Solution GmbH.

Markus Meyer	Fabian Meyer	Andreas Seckinger
Co Geschäftsleiter	Co Geschäftsleiter	Leiter Technik

Auftrag erteilt

Ort, Datum _____

20. Anlage

Die konkreten Inhalte der Auftragsbearbeitung müssen vom Auftraggeber festgelegt und in diesem Vertrag dokumentiert werden. Der Auftraggeber ist für die Vollständigkeit dieser Anlage verantwortlich.

Gegenstand der Bearbeitung

- IT-Dienstleistungen
- Hosting
- Fernwartung

Art und Zweck der Bearbeitung

- Einsichtnahme zum Zwecke der Erbringung von IT-Support -Leistungen
- Einsichtnahme, Veränderung, Vervielfältigung im Rahmen der Fernwartung
- Vervielfältigung zum Zwecke der Durchführung von Datensicherungen und Backups
- Speicherung zum Zwecke des Hostings von Datenbanken und Software

Kategorien von Personendaten

- Personenstammdaten (z.B. Anrede, Name, Anschrift)
- Kommunikationsdaten (z.B. E-Mail-Adresse)
- Verbindungsdaten (z.B. IP-Adresse, ein- und ausgehende Anrufe und E-Mails)
- Allgemeine Vertragsdaten (z.B. Kundennummer, Vertragsgegenstand, Fristen, Bankverbindung, Rechnungsnummer, Ansprechpartner)
- Meldedaten im Beschäftigtenkontext (z.B. Krankheitstage, Urlaubstage. Sozialversicherungsdaten, Mutterschutz. Wiedereingliederung, Vertragslaufzeit)
- Personalzeiterfassung (z.B. Betreten und Verlassen der Arbeitsstätte, Arbeitszeit, An- und Abwesenheit)

Kategorien betroffener Personen

- Kunden
- Lieferanten
- Dienstleister
- Dritte
- Sonstige Geschäftspartner
- Mitarbeiter
- Angehörige von Mitarbeitern

Beschreibung der technischen und organisatorischen Massnahmen

Folgende technische und organisatorische Massnahmen werden durch die

Computer Trend IT-Solution GmbH
Steinengraben 55
CH-4051 Basel

zur Gewährleistung eines angemessenen Datenschutzniveaus ergriffen

1. Massnahmen zur Gewährleistung der Vertraulichkeit (Art. 2 lit. a) DSV, Art. 3 Abs. 1 DSV)

Diese Massnahmen stellen sicher, dass berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen.

- Sichere Löschung von Datenträgern vor deren externer Weitergabe (Verkauf, Leasingrückgabe etc.)
- Ordnungsgemässe Vernichtung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Einsatz von Aktenvernichtern
- Anzahl der Administratoren auf das Mindestmass reduzieren
- Berechtigungskonzept
- Verwaltung der Benutzerrechte durch Systemadministratoren

1.1. Zugangskontrolle (Art. 3 lit. b) DSV)

Diese Massnahmen gewährleisten, dass nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (z.B. Netzwerk, Betriebssystem, Endgerät). Unbefugten ist der Zugang zu verwehren.

- Schliesssystem vorhanden
- Schlüsselverwaltung / Schlüsselbuch
- Videoüberwachung der Zugänge

1.2. Benutzerkontrolle (Art. 3 Abs. 1 lit. c) DSV)

Diese Massnahmen gewährleisten, dass unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können.

- Einsatz von Software gegen Viren oder Spyware
- Regelmässige Kontrolle von Berechtigungen (z.B. Sperrung von Berechtigungen aufgrund von Personalwechsel oder neuen Aufgabenzuteilungen)
- Sensibilisierung des Personals für Phishing-Methoden

2. Massnahmen zur Sicherstellung der Integrität (Art. 2 lit. c) DSV)

Diese Massnahmen stellen sicher, dass Personendaten nicht unberechtigt oder unbeabsichtigt verändert werden.

2.1. Datenträgerkontrolle

Diese Massnahmen gewährleisten, dass unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können.

- Verschlüsseltes externes Backup
- Ordnungsgemässes Vernichten von Datenträgern

2.2. Speicherkontrolle

Diese Massnahmen stellen sicher, dass keine unbefugte Personen Personendaten nicht inkorrekt speichern, lesen, ändern, löschen oder vernichten können.

- Protokollierung von Zugriffen auf Anwendungen
- Festlegen von differenzierten Zugriffsberechtigungen

2.3. Transportkontrolle

Mittels dieser Massnahmen stellen wir sicher, dass unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten könnten.

- Einrichtung von VPN-Verbindungen
- E-Mail-Verschlüsselung
- Sicherstellen, dass nur berechtigte Empfänger Daten erhalten

3. Verfügbarkeit (Art. 2 lit. b) DSV)

Diese Massnahmen beschreiben, wie wir vorgehen, um sicherzustellen, dass die bearbeiteten Personendaten stets verfügbar sind.

3.1. Wiederherstellung

Diese Massnahmen gewährleisten, dass die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

- Datensicherungen
- Wiederherstellungs-System
- Ausarbeiten eines Backup-Konzepts
- IT-Notfallplan (geschäftskritisch)
- Wiederanlaufplan
- Incident Management (IT-Vorfälle, z.B. Befall mit Verschlüsselungstrojaner)

3.2. Verfügbarkeit, Zuverlässigkeit, Datenintegrität

Mittels dieser Verfahren werden wir sicherstellen, dass Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Backup- & Recovery-Konzept
- Regelmässige Tests der Datenwiederherstellung
- IT-Notfallplan
- Serverräume über der Wassergrenze
- SLAs für Verfügbarkeit (Garantien der Verfügbarkeit von Dienstleistern und Vorlieferanten)

3.3. Systemsicherheit

Gewährleisten, dass Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden.
Es geht um die proaktive Behebung von Schwachstellen, für die das System bisher keine Verletzung der Datensicherheit festgestellt hat.

- RMM-Tool für Vulnerability- und Patchmanagement

4. Nachvollziehbarkeit (Art. 2 lit. d) DSV)

Personendaten müssen nachvollziehbar bearbeitet werden.
Dadurch sollen unbefugte Zugriffe oder sogar Missbräuche identifiziert und die Ursache eines Vorfalls ermittelt werden können. Es ist sicherzustellen, dass Aufzeichnungen der Ereignisse und Datenspuren (Beweismittel) erstellt und nicht verändert werden können. Es sollen Verfahren entwickelt werden, um die Wirksamkeit der ergriffenen Massnahmen regelmässig zu kontrollieren, analysieren und zu beurteilen.

4.1. Eingabekontrolle

Mit diesem Massnahmen legen wir fest, dass überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem (Anwendungen / Software) eingegeben oder verändert werden und wie allfällige Änderungen nachvollzogen werden können.

- Protokollierung der Eingabe, Änderung und Löschung von Daten (z.B. Datenbank-Logging, Historie)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Übersicht, mit welchen Anwendungen welche Daten eingegeben, geändert und gelöscht werden können
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

4.2. Erkennung und Beseitigung

Mittels dieser Massnahmen gewährleisten wir, dass Verletzungen der Datensicherheit rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können. Es geht insbesondere um reaktive Massnahmen.

- Sicherheitsvorfälle lösen Alarm aus (Intrusion Detection System, Virenschutz, Alarmanlage)
- Isolierung kompromittierter Systeme
- Notfallhandbuch und/oder Notfallkonzept
- Definition und Einübung von Melde- und Entscheidungswegen und Prozessen
- Dokumentation von Vorfällen
- Spezielle Schulungen für sicherheitsrelevante Themen

4.3. Datenschutzfreundliche Voreinstellungen

Die folgenden Massnahmen stellen sicher, dass durch Voreinstellungen grundsätzlich nur Personendaten, deren Bearbeitung für den jeweiligen bestimmten Bearbeitungszweck erforderlich ist, bearbeitet werden.

- Deaktivierung von datenschutzunfreundlichen Voreinstellungen (kein automatisches GPS-Tracking, kein automatischer Zugriff auf Datenquellen, die für die konkrete Funktion der Software nicht erforderlich sind etc.)
- Nachträgliche Sperrung / Pseudonymisierung / Anonymisierung personenbezogener Daten möglich
- Schnelle Auswertung aller gespeicherten Daten einer betroffenen Person möglich
- Datenschutzfreundliche Gestaltung von Verträgen mit Dienstleistern (Beachtung des Datenminimierungsgrundsatzes bei Gestaltung des Angebots etc.)
- Regelmässige Überprüfung der verwendeten Vertragsmuster in Bezug auf Datenminimierungsgrundsatz
- Organisatorische Beschränkung des Zugriffs auf die personenbezogenen Daten